

# Spectral gap properties of the unitary groups: around Rider's results on non-commutative Sidon sets.

by

Gilles Pisier

Texas A&M University and UPMC-Paris VI

March 14, 2017

## Abstract

We present a proof of Rider's unpublished result that the union of two Sidon sets in the dual of a non-commutative compact group is Sidon, and that randomly Sidon sets are Sidon. Most likely this proof is essentially the one announced by Rider and communicated in a letter to the author around 1979 (lost by him since then). The key fact is a spectral gap property with respect to certain representations of the unitary groups  $U(n)$  that holds uniformly over  $n$ . The proof crucially uses Weyl's character formulae. We survey the results that we obtained 30 years ago using Rider's unpublished results. Using a recent different approach valid for certain orthonormal systems of matrix valued functions, we give a new proof of the spectral gap property that is required to show that the union of two Sidon sets is Sidon. The latter proof yields a rather good quantitative estimate. Several related results are discussed with possible applications to random matrix theory.

MSC: 43A46, 47A56, 22D10

## Contents

1	Notation. Background. Spectral gaps	5
2	The unitary groups	9
3	Rider's results on Sidon sets	17
4	Gaussian and Subgaussian random Fourier series	22
5	Some questions about best constants	36
6	A new approach to Rider's spectral gap	38

A subset  $\Lambda$  of a discrete Abelian group  $\widehat{G}$  is called Sidon if every continuous function on  $G$  with Fourier transform supported in  $\Lambda$  has an absolutely convergent Fourier series.

The study of Sidon sets in discrete Abelian groups was actively developed in the 1970's and 1980's, after Drury's remarkable proof of the stability of Sidon sets under finite unions (see [32]). Rider [47] connected Sidon sets to random Fourier series. This led the author to a new characterization of Sidon sets as  $\Lambda(p)$ -sets (in Rudin's sense) with constants  $O(\sqrt{p})$  and eventually to an arithmetic characterization of Sidon sets (see [37, 34, 39]). Bourgain [1] gave a different proof of this. The 2013 book [18] by Graham and Hare gives an account of this subject, updating the 1975 one [32] by Lopez and Ross. See also [30] for connections with Banach space theory.

Throughout this, the main example always remains the integers  $\widehat{G} = \mathbb{Z}$  (with  $G = \mathbb{T} = \mathbb{R}/\mathbb{Z}$ ), and Sidon sets are defined by the properties of Fourier series on  $\mathbb{T}$  with coefficients supported in the set. The classical example of a Sidon set is a set formed of a sequence  $\{n(k)\}$  such that  $\inf n(k+1)/n(k) > 1$  (such sets are called “Hadamard lacunary”). While the theory was initially inspired by this first example, much of it rests on another one, where  $\mathbb{T}$  is replaced by  $G = \mathbb{T}^{\mathbb{N}}$  (or by  $\{-1, 1\}^{\mathbb{N}}$ ), and the fundamental Sidon set in its dual  $\widehat{G}$  is the one formed by the coordinate functions on  $G$ . In particular, the connections with random Fourier series are closely related to this second example.

Sidon sets are the analogue for discrete groups of the so-called “Helson sets” in continuous groups. The latter subject was actively studied in the late 1960's and 1970's notably by Kahane and Varopoulos in Orsay, Körner in Cambridge and many more (see [25, 26, 19]). Indeed, Sidon sets were then quite popular in harmonic analysis: in the Polish school following an old tradition (Banach, Kaczmarz, Steinhaus, Hartman,...), in the US after Hewitt and Ross, but also in the Italian (around Figà-Talamanca) and Australian schools (around Edwards and Gaudry).

The harmonic analysis of thin sets was extended already in the late 1960's to subsets of the dual “object”  $\widehat{G}$  of any non-commutative compact group  $G$ , with Fourier series replaced by the Peter-Weyl orthogonal development of functions on  $G$ . In this setting pioneering work was done by Figà-Talamanca and Rider ([15, 16, 12]) on generalized random Fourier series. There was initially a lot of excitement around the opening that non-commutative compact groups offered as a substitute for  $\mathbb{T}$ . However, the subject was given a cold shower when it was discovered (see [48, 49, 8, 24]) that even for the simplest example  $G = SU(2)$  infinite Sidon sets do not exist. Since finite Sidon sets were considered trivial, this brought this whole direction to a full stop and probably gave a bad reputation to Sidon sets in the duals of non-commutative compact groups. After that, many in the next generation of researchers, in particular in the Polish school (Bożejko, Pytlik, Szwarz,...) and the Italian one (Figà-Talamanca, Picardello...), turned to harmonic analysis on free groups (see e.g. [13, 14]). In this setting free sets, or “almost free” sets, such as the so-called Leinert sets (see e.g. [29]) or  $L$ -sets in the sense of [42], can be viewed as analogous in some sense to Sidon sets in discrete non-commutative groups.

This context probably explains why Rider, when he published in [47] his theorem connecting Sidon sets and random Fourier series decided not to include the details on the proof of the same result for subsets of the duals of non-commutative compact groups. In the commutative case, full details could be included without any special technical difficulty because the key ingredient was a variant of Drury's interpolation trick (by then well known), invented to prove that the union of two Sidon sets is Sidon, and actually Rider's theorem could be viewed as a generalization of Drury's union theorem. However, the extension of the latter to the non-commutative case was far from obvious (see Remark 1.11), and in fact it was still open until Rider's [47]. Nevertheless, Rider chose to only announce there that he had settled it and promised to include the details, which involved a delicate estimate based on Weyl's character formula for the unitary groups (see Theorem 2.1), in a later publication, but he never did.

In the late 1970's the author proved a series of results on Sidon sets all based initially on Rider's breakthrough from [47]. It turned out that essentially all these results could be extended for subsets of  $\widehat{G}$  when  $G$  is a non-commutative compact group [34, 38]. However, the latter extension required the non-commutative unpublished version of Rider's [47]. At the author's request at the time, Rider kindly communicated to him a detailed handwritten proof of his key result in the non-commutative case. Unfortunately, although a copy of this letter was kept for a long time, it seems now to have been lost. Perhaps the successive moves of the Jussieu Math. Inst. are an excuse, but the guilt is on the author. The more so since Daniel Rider passed away in 2008.

The main goal of this paper is to present the details of a proof of Rider's Theorem for subsets of  $\widehat{G}$  when  $G$  is a general (a priori non-commutative) compact group. Toward the end we give another proof, quite different, that we recently obtained in a more general framework not requiring any group structure.

The main point of Rider's proof is a spectral gap property of the family  $\{U(n) \mid n \geq 1\}$  formed of *all* the unitary groups. The property involves the embedding  $U(n) \rightarrow U(2n)$  obtained by adding 1's on the main diagonal, but the relevant estimate has to be uniform over  $n$ . We feel that this property is of independent interest, likely to find applications in random matrix theory, now that the latter field has become part of the main stream (much more so now than 40 years ago !).

This motivated us to include the full details of (what most likely was) Rider's proof. We then describe in §3 how Rider derived from his spectral gap result the stability of Sidon sets under finite unions and the fact the Sidon property is equivalent to a weaker one involving random Fourier series that we name "randomly Sidon".

In §4 we survey the non-commutative results that we obtained in the 1980's using Rider's unpublished work. Actually we take special care and give detailed proofs because we detected some exaggerated claims there (in [38]) that we no longer believe are true. See Remark 4.14.

In §5, we single out several natural inequalities for random unitaries, related to the classical ones of Khintchine for random signs. We review what is known and discuss the problem of finding the best constants for these.

We seize this occasion to try to revive a bit the whole subject of Sidon sets in duals of non-Abelian compact groups in the light of the recent surge of interest in random matrix theory and Voiculescu's free probability (see [60]). Indeed, although finite sets  $\Lambda \subset \widehat{G}$  are a trivial example of Sidon set, in the non commutative setting one is led to consider sequences of compact groups  $(G_n)$  and sequences of subsets  $\Lambda_n \subset \widehat{G}_n$  with uniformly bounded Sidon constants. Then even if the cardinality of the subsets  $\Lambda_n$  is uniformly bounded (and in fact even if it is equal to 1 !) the notion is interesting. The simplest (and prototypical) example of this situation with  $|\Lambda_n| = 1$  is the case when  $G_n = U(n)$  the group of unitary  $n \times n$ -matrices, and  $\Lambda_n$  is the singleton formed of the irreducible representation (in short irrep) defining  $U(n)$  as acting on  $\mathbb{C}^n$ . Sets of this kind and various generalizations were tackled early on by Rider under the name "local lacunary sets" (see [50]), but we suspect that this setting of sequences of groups, with uniform estimates, which is nowadays commonly accepted, was viewed as not so natural at the time.

We illustrate this in Theorem 4.15. There we consider a sequence of compact groups  $G_n$  and a sequence of unitary irreps  $\pi_n \in \widehat{G}_n$  with unbounded dimensions, and we focus on the situation when the singletons  $\{\pi_n\}$  have uniformly bounded Sidon constants. We give several equivalent characterizations of this situation, in terms of the character  $t \mapsto \text{tr}(\pi_n(t))$  of  $\pi_n$ . Surprisingly, this becomes void if one uses a sequence of finite groups, or of groups that are amenable as discrete groups. In that case the dimensions must remain bounded. E. Breuillard opened our eyes to this phenomenon. We refer the reader to the forthcoming paper [5] for more on this.

# 1. Notation. Background. Spectral gaps

Throughout this section, let  $G$  be a compact group. We denote by  $\widehat{G}$  the dual object formed as usual of all the (equivalence classes of) irreducible representations (irreps in short) on  $G$ . We identify two irreps when they are unitarily equivalent. We denote by  $M(G)$  the space of Radon measures on  $G$  equipped as usual with the total variation norm  $\mu \mapsto \|\mu\|_{M(G)} = |\mu|(G)$ .

We denote by  $M_d$  the space of all complex matrices of size  $d \times d$  with the usual operator norm as acting on  $\ell_2^d$ .

We denote by  $U(d) \subset M_d$  the compact group formed of all unitary matrices of size  $d \times d$ .

For any measure  $\mu$  on  $G$  and any irrep  $\pi : G \rightarrow U(d_\pi)$  we define the Fourier transform by

$$(1.1) \quad \widehat{\mu}(\pi) = \int \overline{\pi(t)} \mu(dt) \in M_{d_\pi}.$$

Note that  $\forall \mu_1, \mu_2 \in M(G)$

$$(1.2) \quad \widehat{\mu_1 * \mu_2}(\rho) = \widehat{\mu_1}(\rho) \widehat{\mu_2}(\rho).$$

We denote by  $m_G$  the normalized Haar measure and by  $t_G \in \widehat{G}$  the trivial representation on  $G$ .

We denote  $L_p(G) = L_p(G, m_G)$ . We view  $L_1(G)$  as isometrically embedded in  $M(G)$  via  $f \mapsto f m_G$ . In particular, the Fourier transform of any  $f \in L_1(G)$  is defined as

$$(1.3) \quad \widehat{f}(\pi) = \int \overline{\pi(t)} f(t) m_G(dt).$$

For any  $f \in L_2(G)$  we have (Parseval)

$$\|f\|_2 = \left( \sum_{\rho \in \widehat{G}} d_\rho \text{tr} |\widehat{f}(\rho)|^2 \right)^{1/2},$$

and the Fourier expansion of  $f$  takes the form

$$f = \sum_{\rho \in \widehat{G}} d_\rho \text{tr}({}^t \widehat{f}(\rho) \rho).$$

*Remark.* Note that our definitions of  $\widehat{\mu}$  and  $\widehat{f}$  in (1.1) and (1.3) differ from that of [23], where  $\widehat{\mu}(\pi)$  is defined as  $\int \pi(t)^* \mu(dt)$  and similarly for  $\widehat{f}$ . Thus the Fourier coefficient in the sense of [23] is the transpose of what it is in our sense. The advantage is that we have (1.2) while the convention of [23] requires to reverse the order of the factors on the right hand side of (1.2).

We denote by  $\chi_\pi$  the character of  $\pi$ , i.e. we have  $\chi_\pi(x) = \text{tr}(\pi(x))$  for any  $x \in G$ . A measure  $\mu \in M(G)$  (resp. a function  $f \in L_1(G)$ ) is called *central* if

$$\forall g \in G \quad \mu = \delta_g * \mu * \delta_{g^{-1}}$$

(resp.  $f = \delta_g * f * \delta_{g^{-1}}$ ). Then the Fourier transform  $\widehat{\mu}$  (resp.  $\widehat{f}$ ) is scalar valued, i.e.  $\widehat{\mu}(\pi)$  or  $\widehat{f}(\pi)$  belong to the space of scalar multiples of the identity matrix of size  $d_\pi$ .

Thus the subspace of the central functions in  $L_p$  ( $1 \leq p < \infty$ ) coincides with the closed linear span of the characters  $\{\chi_\pi \mid \pi \in \widehat{G}\}$ .

There is a bounded linear projection  $P$  from  $M(G)$  onto the subspace of all central measures, defined simply by

$$(1.4) \quad P(\mu) = \int \delta_g * \mu * \delta_{g^{-1}} m_G(dg).$$

Clearly  $\|P(\mu)\| \leq \|\mu\|$ . We denote by  $A(G)$  the Banach space formed of those  $f : G \rightarrow \mathbb{C}$  such that  $\sum_{\pi \in \widehat{G}} d_\pi \text{tr}|\widehat{f}(\pi)| < \infty$ , and we equip it with the norm

$$\|f\|_{A(G)} = \sum_{\pi \in \widehat{G}} d_\pi \text{tr}|\widehat{f}(\pi)|.$$

**Definition 1.1** (Sidon sets). A subset  $\Lambda \subset \widehat{G}$  is called Sidon if there is a constant  $C$  such that

$$\|f\|_{A(G)} \leq C\|f\|_{C(G)}$$

for any  $f \in C(G)$  with Fourier transform supported in  $\Lambda$ . More explicitly, this means that for any finitely supported family  $(a_\pi)$  with  $a_\pi \in M_{d_\pi}$  ( $\pi \in \Lambda$ ) we have

$$\sum_{\pi \in \Lambda} d_\pi \text{tr}|a_\pi| \leq C \left\| \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi a_\pi) \right\|_\infty.$$

For any pair  $f, h \in L_2(G)$ , the convolution  $f * h$  belongs to  $A(G)$  and

$$(1.5) \quad \|f * h\|_{A(G)} \leq \|f\|_{L_2(G)} \|h\|_{L_2(G)}.$$

Moreover, we have for any  $f \in A(G)$  and any  $\nu \in M(G)$

$$(1.6) \quad \int f d\nu = \sum_{\pi \in \widehat{G}} d_\pi \text{tr}(\widehat{f}(\pi) \widehat{\nu}(\bar{\pi})) = \sum_{\pi \in \widehat{G}} d_\pi \sum_{i,j \leq d_\pi} \widehat{f}(\pi)_{ij} \widehat{\nu}(\bar{\pi})_{ij}.$$

and hence

$$(1.7) \quad \left| \int f(g) \nu(dg) \right| \leq \|f\|_{A(G)} \sup_{\pi \in \widehat{G}} \|\widehat{\nu}(\pi)\|.$$

More generally, let  $f, h \in L_\infty(G; M_d)$  ( $d \geq 1$ ). We define the convolution  $F = f * h$  using the matrix product in  $M_d$ , so that  $F_{ij} = \sum_k f_{ik} * h_{kj}$ . Let  $x, y$  be in the unit ball of  $\ell_2^d$ . We have then

$$(1.8) \quad \|\langle Fx, y \rangle\|_{A(G)} \leq \|f\|_{L_\infty(G; M_d)} \|h\|_{L_\infty(G; M_d)}.$$

Indeed, this follows easily from (here we use (1.5))

$$\begin{aligned} \|\langle Fx, y \rangle\|_{A(G)} &\leq \sum_k \left\| \sum_i \bar{x}_i f_{ik} \right\|_2 \left\| \sum_j y_j h_{kj} \right\|_2 \leq \left( \sum_k \left\| \sum_i \bar{x}_i f_{ik} \right\|_2^2 \right)^{1/2} \left( \sum_k \left\| \sum_j y_j h_{kj} \right\|_2^2 \right)^{1/2} \\ &= \left( \int \sum_k \left| \sum_i \bar{x}_i f_{ik} \right|_2^2 dm_G \right)^{1/2} \left( \int \sum_k \left| \sum_j y_j h_{kj} \right|_2^2 dm_G \right)^{1/2} \leq \|f\|_{L_2(G; M_d)} \|h\|_{L_2(G; M_d)}. \end{aligned}$$

A fortiori, we obtain by (1.7)

$$(1.9) \quad \left| \int \langle F(g)x, y \rangle \nu(dg) \right| \leq \|f\|_{L_\infty(G; M_d)} \|h\|_{L_\infty(G; M_d)} \sup_{\pi \in \widehat{G}} \|\widehat{\nu}(\pi)\|.$$

Taking the sup over  $x, y$ , we find

$$(1.10) \quad \left\| \int F(g) \nu(dg) \right\|_{M_d} \leq \|f\|_{L_\infty(G; M_d)} \|h\|_{L_\infty(G; M_d)} \sup_{\pi \in \widehat{G}} \|\widehat{\nu}(\pi)\|.$$

**Notation:** Let  $\mathcal{G} = \prod_{\pi \in \widehat{G}} U(d_\pi)$ . Let  $u \mapsto u_\pi \in U(d_\pi)$  denote the coordinates on  $\mathcal{G}$ .

**Definition 1.2** (Randomly Sidon). A subset  $\Lambda \subset \widehat{G}$  is called randomly Sidon if there is a constant  $C$  such that for any finitely supported family  $(a_\pi)$  with  $a_\pi \in M_{d_\pi}$  ( $\pi \in \Lambda$ ) we have

$$\sum_{\pi \in \Lambda} d_\pi \operatorname{tr}|a_\pi| \leq C \int \left\| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi \pi a_\pi) \right\|_\infty m_G(du).$$

Note that in Lemma 4.6 we give a simple general argument showing that replacing the random unitaries  $(u_\pi)$  by standard complex Gaussian random matrices (with the usual normalization) leads to the same notion of “randomly Sidon”.

Clearly Sidon implies randomly Sidon (with the same constant).

We denote by  $\mathcal{P}(G) \subset M(G)$  the set of probability measures on  $G$ .

We say that  $\Lambda \subset \widehat{G}$  is symmetric if  $\bar{\pi} \in \Lambda$  for any  $\pi \in \Lambda$ .

**Definition 1.3** (Spectral gap). Let  $0 \leq \gamma < \delta \leq 1$ . We will say that a probability measure  $\mu \in \mathcal{P}(G)$  has a  $(\delta, \gamma)$ -spectral gap with respect to a symmetric subset  $\Lambda \subset \widehat{G}$  if  $\widehat{\mu}(\pi) = \delta I$  for any  $\pi \in \Lambda$  and  $\|\widehat{\mu}(\rho)\| \leq \gamma$  for any nontrivial  $\rho \notin \Lambda$ .

*Remark 1.4* (Spectral gap as an inequality). Let  $E \subset L_2(G)$  be the subspace formed of those  $f \in L_2(G)$  such that  $\widehat{f}(\pi) = 0$  for any non-trivial  $\pi \notin \Lambda$ . Let  $P : L_2(G) \rightarrow E$  denote the orthogonal projection. Note  $Pf = \int f dm_G + \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}({}^t \widehat{f}(\pi) \pi)$  for any  $f \in L_2(G)$ . Let  $P_\delta f = \int f dm_G + \delta \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}({}^t \widehat{f}(\pi) \pi)$ . Then  $\mu$  has a  $(\delta, \gamma)$ -spectral gap with respect to  $\Lambda$  iff

$$\forall f \in L_2(G) \quad \|\mu * f - P_\delta f\|_2 \leq \gamma \|f - Pf\|_2.$$

**Definition 1.5**  $((\delta, \gamma)$ -isolated). We will say that  $\Lambda \subset \widehat{G}$  is  $(\delta, \gamma)$ -isolated if there is  $\mu \in \mathcal{P}(G)$  that has a  $(\delta, \gamma)$ -spectral gap with respect to  $\Lambda$ .

*Remark 1.6.* Using the central projection (1.4) we may always assume in the preceding that  $\mu$  is a central measure.

The basic example is the set  $\Lambda = \{-1, 1\} \subset \mathbb{Z}$ . The measure  $\mu = (1 + \cos(t))m_{\mathbb{T}}(dt)$  has a  $(1/2, 0)$ -spectral gap with respect to  $\Lambda$ .

On  $G = \{-1, 1\}$  the measure  $\mu = (1 + \xi)m_G$  does the same with respect to the set formed of the character  $\xi \in \widehat{G}$  associated to the identity map.

More generally, Riesz products give more sophisticated examples. Let  $G$  be a compact Abelian group. Let  $\{\gamma_n \mid n \in \mathbb{N}\} \subset \widehat{G}$  be “quasi-independent”, i.e. such that there is no nontrivial choice of  $(\xi_n) \in \{-1, 0, 1\}^{\mathbb{N}}$  finitely supported such that  $\prod \gamma_n^{\xi_n} = 1$ . Assume  $-1 \leq \delta_n \leq 1$ . Then the probability measures  $\nu_k = \prod_{n \leq k} (1 + \delta_n \Re(\gamma_n))m_G$  converge weakly when  $k \rightarrow \infty$  to a probability  $\nu$  on  $G$ . We refer to  $\nu$  as the Riesz product associated to  $\prod (1 + \delta_n \Re(\gamma_n))$ .

If we assume that  $\delta_n = \delta$  for all  $n$  and  $0 < \delta < 1$ , then the Riesz product  $\nu$  has a  $(\delta, \delta^2)$ -spectral gap with respect to  $\Lambda = \{\gamma_n\} \cup \{\bar{\gamma}_n\}$ . For instance, this holds for  $G = \mathbb{R}/2\pi\mathbb{Z}$  when  $\Lambda = \{\gamma_n\}$  is identified to the subset  $\{2^n\} \subset \mathbb{Z}$  by  $\gamma_n(t) = \exp(i2^n t)$ . This also holds for  $G = \{-1, 1\}^{\mathbb{N}}$  (resp.  $G = \mathbb{T}^{\mathbb{N}}$ ) when  $\Lambda \subset \widehat{G}$  is the set  $\{\xi_n\}$  (resp.  $\{\xi_n\} \cup \{\bar{\xi}_n\}$ ) with  $(\xi_n)$  denoting the coordinates on  $G$ .

Let  $\sigma_n : U(n) \rightarrow M_n$  be the “defining” irrep, i.e. the identity map on  $U(n)$ .

**Lemma 1.7.** Let  $n \geq 1$ . For any  $0 < \delta \leq 1/(2n)$ , let

$$\varphi_n^\delta = 1 + \delta(\chi_{\sigma_n} + \overline{\chi_{\sigma_n}}) = 1 + \delta(\operatorname{tr}(\sigma_n) + \overline{\operatorname{tr}(\sigma_n)}).$$

Let  $\nu_n^\delta \in M(U(n))$  be the probability measure defined by  $\nu_n^\delta = \varphi_n^\delta m_{U(n)}$ . Then  $\nu_n^\delta$  has a  $(\delta/n, 0)$ -spectral gap with respect to  $\{\sigma_n, \overline{\sigma_n}\}$ .

*Proof.* Obviously  $\widehat{\varphi_n^\delta}(\sigma_n) = \widehat{\varphi_n^\delta}(\overline{\sigma_n}) = \delta/n$  and  $\widehat{\varphi_n^\delta}(\pi) = 0$  for any other nontrivial irrep  $\pi$ .  $\square$

**Definition 1.8** (peak sets). Let  $0 < \varepsilon < 1$ . We say that  $\Lambda \subset \widehat{G}$  is an  $\varepsilon$ -peak set with constant  $w$  if there is  $\nu \in M(G)$  with  $\|\nu\|_{M(G)} \leq w$  such that  $\widehat{\nu}(\pi) = I$  for any  $\pi \in \Lambda$  and  $\sup_{\rho \notin \Lambda} \|\widehat{\nu}(\rho)\| \leq \varepsilon$ .

*Remark 1.9.* If  $\nu$  is as in Definition 1.8 for some  $0 < \varepsilon < 1$  then  $\nu^{*k}$  satisfies the same with  $\varepsilon^k, w^k$  in place of  $\varepsilon, w$ . Therefore, if  $\Lambda$  is an  $\varepsilon$ -peak set for some  $0 < \varepsilon < 1$ , then it is so for all  $0 < \varepsilon < 1$ .

**Definition 1.10** (peaking Sidon sets). We say that a Sidon set  $\Lambda \subset \widehat{G}$  is peaking if for any  $0 < \varepsilon < 1$  and any  $u \in \mathcal{G}$  (or merely for any  $u \in \prod_{\pi \in \Lambda} U(d_\pi)$ ) there is a measure  $\mu_\varepsilon^u \in M(G)$  such that

$$\widehat{\mu_\varepsilon^u}(\pi) = u_\pi \quad \forall \pi \in \Lambda, \quad \sup_{\pi \notin \Lambda} \|\widehat{\mu_\varepsilon^u}(\pi)\| \leq \varepsilon \text{ and } \|\widehat{\mu_\varepsilon^u}\| \leq w(\varepsilon)$$

where  $w(\varepsilon)$  depends only on  $\varepsilon$ .

*Remark 1.11* (The main difficulty of the non-Abelian case). Note that one of our main goals will be to prove that actually any Sidon set is peaking. This will be reached in Theorem 3.5 and Remark 3.9. Once this goal is attained, it follows as an easy corollary that the union of two Sidon sets is also one (see Corollary 3.6). In the Abelian case, Drury's (or Rider's) proof made crucial use of the Riesz product  $\prod(1 + \delta(z_n + \bar{z}_n)/2)$  on  $\mathbb{T}^\mathbb{N}$  ( $0 \leq \delta < 1$ ). With the notation in Lemma 1.7 this is the same as the infinite product of the probability  $\nu_1^\delta$  on  $\mathbb{T}$ . The latter has a  $(\delta, \delta^2)$ -spectral gap with respect to the Sidon set formed of the coordinates on  $\mathbb{T}^\mathbb{N}$ , which is the fundamental example in the Abelian case. The proof that Sidon sets are peaking uses a certain transplantation trick due to Drury to pass from the fundamental example to the general case. It is not really difficult to adapt that trick to the non-Abelian case (see the proof of Theorem 3.5). However, in the non-Abelian case the fundamental example is the product  $\prod_{n \geq 1} U(n)$  but the product of the probabilities  $\nu_n^\delta$  fails to have the required spectral gap, whence the need for a substitute for the Riesz product. This is precisely the role of Theorem 2.1 in the next section.

The preceding definitions are connected by the following simple result.

**Proposition 1.12.** *Let  $0 < \gamma < \delta < 1$ . Any  $(\delta, \gamma)$ -isolated symmetric set  $\Lambda \subset \widehat{G}$  is an  $\varepsilon$ -peak set with constant  $w$  for some  $0 < \varepsilon < 1$  and  $w \geq 0$  depending only on  $\gamma, \delta$ .*

*Any Sidon set  $\Lambda \subset \widehat{G}$  that is also an  $\varepsilon$ -peak set with constant  $w$  for some  $0 < \varepsilon < 1$  and  $w \geq 0$  is peaking.*

*Proof.* Let  $\mu$  be as in Definition 1.3. Let  $\nu = \delta^{-1}(\mu - m_G)$  with  $\varepsilon = \gamma/\delta$  and  $w = d^{-1}(\|\mu\| + 1)$ . Then  $\nu$  satisfies the property in Definition 1.8. If  $\Lambda$  is Sidon with constant  $C$ , by (i) in Lemma 3.3 (Hahn-Banach), for any  $u \in \mathcal{G}$  there is a measure  $\mu^u \in M(G)$  such that

$$\widehat{\mu^u}(\pi) = u_\pi \quad \forall \pi \in \Lambda \text{ and } \|\widehat{\mu^u}\| \leq C.$$

Let  $\nu$  be as in Definition 1.8. Then  $\mu_\varepsilon^u = \mu^u * \nu$  is as in Definition 1.10 with  $w(\varepsilon) = Cw$ . This gives the announced result for some  $0 < \varepsilon < 1$ , but replacing  $\nu$  by its convolution powers we obtain a similar result for any  $0 < \varepsilon < 1$ .  $\square$

**Proposition 1.13.** *Let  $G = \prod_{n \in \mathbb{N}} G_n$  be the product of a sequence of compact groups, let  $(\mu_n)$  be a sequence with  $\mu_n \in \mathcal{P}(G_n)$  and let  $(\Lambda_n)$  be a sequence of symmetric subsets with  $\Lambda_n \subset \widehat{G_n}$  for each  $n$ . Let  $0 < \gamma < \delta < 1$ . Let  $\gamma' = \max\{\gamma, \delta^2\} < \delta$ . If  $\mu_n$  has a  $(\delta, \gamma)$ -spectral gap with respect to  $\Lambda_n$  for each  $n$ , then the product  $\mu = \otimes_{n \in \mathbb{N}} \mu_n$  has a  $(\delta, \gamma')$ -spectral gap with respect to the subset  $\Lambda \subset \widehat{G}$ , denoted by  $\dot{\Sigma}\Lambda_n$ , consisting of all the irreps  $\pi$  on  $G$  of the following form: for some  $n$  there is  $\pi_n \in \Lambda_n$  such that*

$$\forall x = (x_n) \in G \quad \pi(x) = \pi_n(x_n).$$



*Proof.* Let  $\pi \in \dot{\Sigma}\Lambda_n$ . Then  $\widehat{\mu}(\pi) = \widehat{\mu_n}(\pi_n)$ . Any nontrivial  $\pi \in \widehat{G}$  is of the form  $\pi(x) = \otimes_{n \in \mathbb{N}} \pi_n(x_n)$  for some sequence  $(\pi_n)$  with  $\pi_n \in \widehat{G_n}$  containing some but only finitely many nontrivial terms. If at least one of these non trivial terms  $\pi_n$  is not in  $\Lambda_n$ , then  $\|\widehat{\mu}(\pi)\| \leq \gamma$ . If they are all in  $\Lambda_n$  and  $\pi \notin \Lambda$ , there must be at least two of them and then  $\|\widehat{\mu}(\pi)\| \leq \delta^2$ . The result is then immediate.  $\square$

*Remark 1.14.* Let  $G_k = U(d_k)$  and  $G = \prod G_k$ . Assume that  $N = \sup_k d_k < \infty$ . Let  $0 < \delta \leq 1/(2N)$ . Let  $\varphi_n \in L_1(G)$  be defined for  $x = (x_k) \in G$  by  $\varphi_n(x) = \prod_{k \leq n} (1 + \delta(\text{tr}(x_k) + \text{tr}(\overline{x_k})))$ , and let  $\nu_n = \varphi_n m_G$ . As for Riesz products,  $\nu_n \in \mathcal{P}(G)$ ,  $\nu_n$  converges weakly to some  $\nu \in \mathcal{P}(G)$ , and it is easy to check, similarly, that  $\nu$  has a  $(\delta/N, \delta^2/N^2)$ -spectral gap. This can also be seen as a particular case of the preceding Proposition with  $\gamma = 0$  and  $\delta$  replaced by  $\delta/N$ .

## 2. The unitary groups

The main difficulty Rider had to overcome to establish his main result is the following spectral gap (and interpolation) property of the sequence of the unitary groups  $\{U(n) \mid n \geq 1\}$ , which in our opinion, is quite deep. Note however that, for the applications to Sidon sets, any probability with the same gap property as the one denoted below by  $\nu_n$  would do (see §6).

Let  $1 \leq k \leq n$ . Let  $\Gamma(k) \subset U(n)$  be the copy of  $U(k)$  embedded in  $U(n)$  via  $a \mapsto a \oplus I$ . Let  $\mu_{k,n}$  be the central symmetric probability measure defined by

$$(2.1) \quad \mu_{k,n} = \int \delta_s * m_{\Gamma(k)} * \delta_{s^{-1}} m_{U(n)}(ds).$$

We denote by  $\sigma_n \in \widehat{U(n)}$  the defining representation of  $U(n)$ .

We denote by  $S_n \subset \widehat{U(n)}$  the set

$$S_n = \{\sigma_n, \overline{\sigma_n}\}.$$

For emphasis : it is crucial in the next statement that  $\gamma < 1/2$  be *independent of*  $n$ .

**Theorem 2.1.** [*Rider, circa 1975, unpublished*]

For any even  $n \geq 2$ , let  $k = n/2$  and let  $\nu_n = \mu_{k,n}$ .

For any odd  $n$ , let  $k_+ = n/2 + 1/2$ ,  $k_- = n/2 - 1/2$  and  $\nu_n = 1/2(\mu_{k_-,n} + \mu_{k_+,n})$ .

There is a positive constant  $\gamma < 1/2$  such that for any  $n \geq 4$ , the symmetric central probability measure  $\nu_n$  has a  $(1/2, \gamma)$ -spectral gap with respect to  $S_n$ . More precisely, for any  $1/4 < \gamma < 1/2$  this holds for all sufficiently large  $n$ .

*Remark 2.2.* The case  $n = 1$ ,  $G = \mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$  is classical. Then the probability measure

$$\mu(dt) = (1 + \cos t) m_{\mathbb{T}}(dt)$$

(which is the building block for Riesz products) satisfies the analogous interpolation property, with  $\gamma = 0$ .

**Corollary 2.3.** Let  $(d_k)_{k \in I}$  be an arbitrary collection of integers. Let  $G = \prod_{k \in I} U(d_k)$ . Let  $S \subset \widehat{G}$  be the subset formed of all representations  $\pi$  that, for some  $k \in I$ , are of the form  $\pi(g) = \sigma_{d_k}(g_k)$  ( $g \in G$ ). For any  $0 < \varepsilon < 1$  there is a measure  $\mu_\varepsilon \in M(G)$  such that

$$\widehat{\mu}_\varepsilon(\pi) = I \quad \forall \pi \in S, \quad \sup_{\pi \notin S} \|\widehat{\mu}_\varepsilon(\pi)\| \leq \varepsilon \quad \text{and} \quad \|\mu\| \leq w(\varepsilon)$$

where  $w(\varepsilon)$  depends only on  $\varepsilon$ .

*Proof.* By Theorem 2.1, there is  $N$  (e.g.  $N = 4$ ) and  $0 < \gamma < 1/2$  such that  $S_n$  has a  $(1/2, \gamma)$ -spectral gap for any  $n \geq N$ . Let  $G = G_1 \times G_2$  with  $G_1 = \prod_{d_k < N} U(d_k)$  and  $G_2 = \prod_{d_k \geq N} U(d_k)$ . Let  $S_1 \subset \widehat{G_1}$  and  $S_2 \subset \widehat{G_2}$  be the corresponding subsets and let  $\Lambda_j = S_j \cup \overline{S_j}$  ( $j = 1, 2$ ). By Remark 1.14,  $\Lambda_1$  is  $(\lambda, \lambda^2)$ -isolated for any  $0 < \lambda \leq 1/2N$ . We may clearly assume  $\gamma \geq 1/4$ . Then by Proposition 1.13,  $\Lambda_2$  is  $(1/2, \gamma)$ -isolated. Taking convolution powers, we see that it is also  $(1/2^m, \gamma^m)$ -isolated for any integer  $m \geq 1$ . Choose  $m$  minimal but large enough so that  $1/2^m \leq 1/(2N)$ . Let  $\delta = 1/2^m$  and  $\gamma' = \max\{\gamma^m, \delta^2\}$ . Then both  $\Lambda_1$  and  $\Lambda_2$  are  $(\delta, \gamma')$ -isolated. Therefore, by Proposition 1.13  $S \cup \bar{S}$  is also  $(\delta, \gamma')$ -isolated. By Proposition 1.12,  $S \cup \bar{S}$  is an  $\varepsilon$ -peak set for some  $0 < \varepsilon < 1$ . Let  $\nu_1 \in M(G)$  be such that  $\widehat{\nu}_1 = I$  on  $S \cup \bar{S}$  but  $\|\widehat{\nu}_1\| \leq \varepsilon$  outside  $S \cup \bar{S}$ . It remains to show the same but with  $S$  in place of  $S \cup \bar{S}$ . For any  $z \in \mathbb{T}$ , let  $Z(z) \in G$  be the element such that  $Z(z)_k = zI_k$ . Note  $\widehat{\delta_{Z(z)}}(\sigma_k) = \bar{z}I_k$ . Then let

$$\nu_2 = \int z(\delta_{Z(z)} * \nu_1) m_{\mathbb{T}}(dz).$$

Now  $\widehat{\nu}_2 = I$  on  $S$ , and  $\widehat{\nu}_2 = 0$  on  $\bar{S}$ . Also  $\|\widehat{\nu}_2\| \leq \|\widehat{\nu}_1\|$  on all of  $\widehat{G}$ . Thus  $\|\widehat{\nu}_1\| \leq \varepsilon$  outside  $S$  and  $\|\nu_2\| \leq \|\nu_1\|$ . By Remark 1.9 this completes the proof.  $\square$

We will need some background on irreps of the unitary groups. The ultraclassical reference is Hermann Weyl's [62]. See e.g. [45, 52, 55] for more recent accounts on the combinatorics of this rich subject. We greatly benefitted from the expositions in [11] and [17].

Recall that for any compact group  $G$ , the set  $\widehat{G}$  consists of irreps on  $G$  with exactly one representative, up to unitary equivalence, of each irrep. Let  $G = U(n)$ . Then  $\widehat{G}$  is in 1-1 correspondence with the set of  $n$ -tuples  $m = (m_1, m_2, \dots, m_n)$  in  $\mathbb{Z}^n$  such that  $m_1 \geq \dots \geq m_n$ . Let  $t = (t_1, \dots, t_n) \in \mathbb{C}^n$ . Let  $A_m(t)$  denote the determinant of the  $n \times n$ -matrix  $a_m(t)$  defined by

$$a_m(t)_{ij} = t_i^{m_j}.$$

Let  $\delta = (n-1, n-2, \dots, 1, 0)$ . Let  $\pi_m$  be the irrep corresponding to  $m$ , and let  $\chi_m$  denote its character. Then for any unitary  $g \in U(n)$  with eigenvalues  $t = (t_1, \dots, t_n) \in \mathbb{T}^n$ ,  $g$  is unitarily equivalent to the diagonal matrix  $D(t)$  with coefficients  $t$ . This implies that  $\chi_m(g) = \text{tr}(\pi_m(g)) = \text{tr}(\pi_m(D(t))) = \chi_m(D(t))$ . For simplicity, we will identify  $t$  with  $D(t)$  and we set  $\chi_m(t) = \chi_m(D(t))$ . We can now state Weyl's fundamental character formula, which goes back to [62]:

$$(2.2) \quad \chi_m(t) = \frac{A_{m+\delta}(t)}{A_\delta(t)}.$$

Note that  $A_\delta(t)$  is but the classical Vandermonde determinant

$$A_\delta(t) = \prod_{i < j} (t_i - t_j).$$

We observe that for any  $d \in \mathbb{Z}$  we have

$$A_{m+(d, \dots, d)}(t) = (t_1 t_2 \dots t_n)^d A_m(t)$$

and hence for any  $g \in G$

$$\chi_{m+(d, \dots, d)}(g) = \det(g)^d \chi_m(g).$$

Thus if we choose  $d = -m_n$ , and set  $\lambda_j = m_j + d$ , we have  $\lambda_1 \geq \dots \lambda_{n-1} \geq \lambda_n = 0$ , and

$$(2.3) \quad \chi_m(g) = \det(g)^{m_n} \chi_\lambda(g).$$

*Remark 2.4.* [Distinguished representations of  $U(n)$ ] The trivial representation of  $U(n)$  corresponds to  $m_1 = \dots = m_n = 0$ , so that  $d = 0$  and  $\lambda_1 = \dots = \lambda_n = 0$ , and then  $\chi_m(t) = 1$  for all  $t \in U(n)$ . The representation  $\sigma_n(t) = t$  corresponds to  $m = \lambda = (1, 0, \dots, 0)$  and  $d = 0$ . Then

$$\chi_m(t) = t_1 + \dots + t_n.$$

The representation  $\sigma_n(t) = \bar{t}$  corresponds to  $m = (0, \dots, 0, -1)$  or equivalently to  $\lambda = (1, \dots, 1, 0)$  and  $d = 1$ . Then

$$\chi_m(t) = \bar{t}_1 + \dots + \bar{t}_n = \left( \prod_{j \neq 1} t_j + \dots + \prod_{j \neq n} t_j \right) \det(t)^{-1}.$$

In the sequel, we denote

$$\lambda_+ = (1, 0, \dots, 0) \quad \text{and} \quad \lambda_- = (1, \dots, 1, 0).$$

The point of (2.3) is that now  $\lambda$  can be identified with a Young diagram with a first row of  $\lambda_1$  boxes, sitting as usual above a second row of  $\lambda_2$  boxes, and so on. This will allow us to take advantage of the so-called Jacobi-Trudi formula (see [17, p. 75]) :

$$(2.4) \quad \chi_\lambda(t) = s_\lambda(t),$$

where  $s_\lambda$  is the famous Schur symmetric polynomial in  $t = (t_1, \dots, t_n)$ , which can be defined for  $\lambda \neq 0$  as the sum

$$(2.5) \quad s_\lambda(t) = \sum t^T$$

running over all the admissible fillings (or “tableaux”)  $T$  of the diagram  $\lambda$  with the numbers  $1, 2, \dots, n$ . Here an admissible filling assigns to any box a number in  $1, 2, \dots, n$  so that the numbers are strictly increasing when running down a column and weakly increasing along each row, and

$$t^T = \prod_{1 \leq i \leq n} t_i^{r_i}$$

where  $r_i \geq 0$  is the number of times  $i$  is used in the filling  $T$ .

By convention, for the case  $\lambda_1 = \dots = \lambda_n = 0$ , we set  $s_0(t) = 1$ .

Let  $1^n = (1, \dots, 1)$  where 1 is repeated  $n$  times. Then (2.5) implies

$$(2.6) \quad s_\lambda(1^n) = |\{T\}|,$$

i.e.  $s_\lambda(1^n)$  is the number of admissible fillings of  $\lambda$  with the numbers  $1, 2, \dots, n$ .

Then for any  $\lambda = (\lambda_1, \dots, \lambda_n)$  with  $\lambda_1 \geq \dots \geq \lambda_n \geq 0$  we have

$$(2.7) \quad \chi_\lambda(1^n) = s_\lambda(1^n) = \prod_{i < j} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

Note that  $\frac{\lambda_i - \lambda_j + j - i}{j - i} \geq 1$  for all  $i < j$ .

This classical formula can be deduced from (2.2): by setting  $t = (1, x, x^2, \dots, x^{n-1})$ , and observing that  $A_{\lambda+\delta}(1, x, x^2, \dots, x^{n-1})$  is a Vandermonde determinant, we have

$$\chi_\lambda(1, x, x^2, \dots, x^{n-1}) = x^{\sum (i-1)\lambda_i} \prod_{i < j} \frac{x^{\lambda_i - \lambda_j + j - i} - 1}{x^{j-i} - 1}.$$

Then letting  $x$  tend to 1, and making the obvious common division in numerator and denominator, (2.7) follows.

The preceding definition of the Schur symmetric polynomial  $s_\lambda$  is classically given as a function of  $k$ -variables with  $k$  not necessarily equal to the number of rows  $n$  of  $\lambda$ : one sets

$$s_\lambda(t_1, \dots, t_k) = \sum t^T$$

where the sum runs over all the admissible fillings of the Young diagram  $\lambda$  by the numbers  $1, 2, \dots, k$ , with  $t^T$  as before.

If  $\lambda_n > 0$  and  $k < n$ , then the first column has length  $> k$ , so there are no admissible fillings by  $(1, \dots, k)$  and  $s_\lambda(t_1, \dots, t_k) = 0$  in that case.

We now fix  $1 \leq k < n$ .

We wish to compute the restriction of  $\chi_\lambda$  to the subgroup  $U(k)$  viewed as embedded in  $U(n)$  via  $a \mapsto a \oplus I$  or equivalently  $a \mapsto \begin{pmatrix} a & 0 \\ 0 & I_{n-k} \end{pmatrix}$ . In other words we are after a formula for  $\chi_\lambda(t_1, \dots, t_k, 1^{n-k})$ .

We find it convenient to use (2.4) and (2.5). Note that any admissible filling of  $\lambda$  by  $(1, \dots, n)$  induces by restricting it to  $(1, \dots, k)$  a filling of a diagram  $\mu \leq \lambda$ , in the sense that  $\mu_i \leq \lambda_i$  for all  $1 \leq i \leq n$ . The remaining set of boxes, denoted by  $\lambda \setminus \mu$  is (in general) no longer a diagram, it is only what is called a skew diagram, but the rule for filling it is respected by the induced numbering on its rows and columns, so that we can extend to  $\lambda \setminus \mu$  the notation (2.5). Thus to any admissible filling of  $\lambda$  by  $(1, \dots, n)$  we associate  $\mu \leq \lambda$  with a filling by  $(1, \dots, k)$  and  $\lambda \setminus \mu$  with a filling by  $(k+1, \dots, n)$ . Conversely, a moment of thought shows that separate admissible fillings of  $\mu$  by  $(1, \dots, k)$  and  $\lambda \setminus \mu$  by  $(k+1, \dots, n)$  can be joined to form a filling of  $\lambda$  by  $(1, \dots, n)$ . This leads to the identity (see [52, p. 175])

$$(2.8) \quad s_\lambda(t) = \sum_{\mu \leq \lambda} s_\mu(t_1, \dots, t_k) s_{\lambda \setminus \mu}(t_{k+1}, \dots, t_n),$$

where again we set by convention  $s_{\lambda \setminus \mu}(t_{k+1}, \dots, t_n) = 1$  if  $\mu = \lambda$ .

Moreover, we write  $\mu \subset \lambda$  when  $\mu_i \leq \lambda_i$  for all  $1 \leq i \leq n$ .

**Lemma 2.5.** *Recall that  $\mu_{k,n}$  is the central symmetric probability measure defined by (2.1). Let  $m = (m_1, \dots, m_n) \in \mathbb{Z}^n$ , and let  $\lambda_j = m_j - m_n$  ( $1 \leq j \leq n$ ). The Fourier transform of  $\mu_{k,n}$  is as follows: If  $m_n > 0$  we have  $\widehat{\mu_{k,n}}(\pi_m) = 0$ .*

*If  $m_n \leq 0$ , let  $d = -m_n$  and let  $[d]^k = (d, \dots, d, 0, \dots, 0)$  with  $d$  repeated  $k$ -times. Then  $\widehat{\mu_{k,n}}(\pi_m) = 0$  unless  $[d]^k \subset \lambda$  in which case we have*

$$(2.9) \quad \widehat{\mu_{k,n}}(\pi_m) = \frac{s_{\lambda \setminus [d]^k}(1^{n-k})}{s_\lambda(1^n)}.$$

*Proof.* We denote by  $(t_1, \dots, t_k, 1^{n-k})$  the eigenvalues of  $g \in \Gamma(k)$ , with  $t = (t_1, \dots, t_k) \in \mathbb{T}^k$ . Then

$$\widehat{\mu_{k,n}}(\pi_m) = \frac{1}{\dim(\pi_m)} F_{k,n}(\pi_m) I$$

where by (2.3)

$$F_{k,n}(\pi_m) = \int \overline{\det(g)^{-d} \chi_\lambda(g)} m_{\Gamma(k)}(dg) = \int (t_1 \cdots t_k)^d \overline{\chi_\lambda(t_1 \cdots t_k, 1^{n-k})} m_{\Gamma(k)}(dg).$$

By (2.8) we have

$$\chi_\lambda(t_1 \cdots t_k, 1^{n-k}) = \sum_{\mu \leq \lambda} s_\mu(t_1, \dots, t_k) s_{\lambda \setminus \mu}(1^{n-k}).$$

Since the characters of  $\Gamma(k)$  are orthonormal in  $L_2(m_{\Gamma(k)})$  the integral

$$\int (t_1 \cdots t_k)^d \overline{s_\mu(t_1, \dots, t_k)} m_{\Gamma(k)}(dg)$$

is  $= 1$  if  $\pi_\mu$  is equivalent to the irrep  $g \mapsto \det(g)^d$  on  $\Gamma(k)$ , and  $= 0$  otherwise.

Since  $g \mapsto \det(g)^d$  on  $\Gamma(k)$  corresponds to  $(d, \dots, d)$  ( $k$ -times) on  $U(k)$ , we have

$$F_{k,n}(\pi) = \sum_{\mu \leq \lambda} \int (t_1 \cdots t_k)^d \overline{s_\mu(t_1, \dots, t_k)} m_{\Gamma(k)}(dg) s_{\lambda \setminus \mu}(1^{n-k}) = s_{\lambda \setminus [d]^k}(1^{n-k}).$$

More precisely,  $\widehat{\mu_{k,n}}(\pi) = 0$  for all  $d < 0$ , and also  $\widehat{\mu_{k,n}}(\pi) = 0$  whenever  $[d]^k \not\leq \lambda$ . Thus, if  $[d]^k \leq \lambda$  and  $0 \leq d \leq \lambda_k$ , we have

$$F_{k,n}(\pi) = s_{\lambda \setminus [d]^k}(1^{n-k}).$$

Moreover

$$(2.10) \quad \dim(\pi_m) = \dim(\pi_\lambda) = \chi_\lambda(1_G) = s_\lambda(1^n).$$

This proves (2.9). □

**Lemma 2.6.** *Let  $1 \leq k < n$ . Let  $\lambda = (\lambda_1, \dots, \lambda_n)$  with  $\lambda_1 \geq \dots \geq \lambda_n = 0$ . Assume  $[d]^k \subset \lambda$  or equivalently  $0 \leq d \leq \lambda_k$ . Let  $\lambda' = (\lambda_1, \dots, \lambda_k) \setminus [d]^k$  and  $\lambda'' = (\lambda_{k+1}, \dots, \lambda_n)$ . Then*

$$s_{\lambda \setminus [d]^k}(1^{n-k}) \leq s_{\lambda'}(1^{n-k}) s_{\lambda''}(1^{n-k}).$$

*We have equality if  $\lambda_{k+1} \leq d$ .*

*Moreover,  $s_{\lambda \setminus [d]^k}(1^{n-k}) = 0$  if  $d < \lambda_{n-k+1}$  (and a fortiori if  $k+1 > n-k$  and  $d < \lambda_{k+1}$ ).*

*Proof.* To any admissible filling of  $\lambda \setminus [d]^k$  we may associate, by restriction, an admissible filling of  $\lambda'$  and one of  $\lambda''$ . Since this correspondence is clearly injective, the inequality follows from (2.6). Equality holds if it is surjective. Consider a pair of separate fillings of  $\lambda'$  and  $\lambda''$ . If  $\lambda_{k+1} \leq d$  there is no problem to join them into a filling of  $\lambda \setminus [d]^k$ , so we have surjectivity. If  $\lambda_{k+1} > d$  there may be an obstruction, however  $s_{\lambda \setminus [d]^k}(1^{n-k}) = 0$  if  $d < \lambda_{n-k+1}$ , because one cannot fill the  $(d+1)$ -th column strictly increasingly by  $1, \dots, n-k$  (that column being of length  $\geq n-k+1$  is too long for that). □

**Lemma 2.7.** *With the same notation as in Lemma 2.6:*

(i) *If  $d = 0$  then  $\widehat{\mu_{k,n}}(\pi_m) = 0$  if  $\lambda_{n-k+1} > 0$ , and*

$$\widehat{\mu_{k,n}}(\pi_m) = \left( \prod_{i < j, j > n-k} \frac{\lambda_i + j - i}{j - i} \right)^{-1} \quad \text{if } \lambda_{n-k+1} = 0.$$

(ii) *If  $d \geq 1$ ,  $[d]^k \subset \lambda$  and  $n-k \leq k$  then*

$$\widehat{\mu_{k,n}}(\pi_m) \leq \left( \prod_{i \leq k < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \right)^{-1}.$$

(iii) *Moreover,  $\widehat{\mu_{k,n}}(\pi_m) = 0$  if  $\lambda_k < d$  or if  $d < \lambda_{n-k+1}$ .*

*Proof.* We will use (2.9). Recall  $\lambda_n = 0$ .

(i) Assume  $d = 0$ . Clearly,  $s_\lambda(1^{n-k}) = 0$  if  $\lambda_{n-k+1} > 0$ , because then we cannot fill the first column. Now assume  $\lambda_{n-k+1} = 0$  ( $= \lambda_n$ ). By (2.7) we have then  $s_\lambda(1^{n-k}) = \prod_{i < j \leq n-k} \frac{\lambda_i - \lambda_j + j - i}{j - i}$ , and hence by (2.9) and (2.7)

$$\widehat{\mu_{k,n}}(\pi_m) = \left( \prod_{i < j, j > n-k} \frac{\lambda_i + j - i}{j - i} \right)^{-1}.$$

(ii) Let  $\mu = [d]^k$ . Note that  $[d]^k \subset \lambda$  implies  $\lambda_k \geq d$ . With the notation of Lemma 2.6, since by (2.6)  $n - k \leq k$  clearly implies  $s_{\lambda'}(1^{n-k}) \leq s_{\lambda'}(1^k)$ , we have

$$s_{\lambda \setminus [d]^k}(1^{n-k}) \leq s_{\lambda'}(1^k) s_{\lambda''}(1^{n-k}).$$

We note that  $\lambda'_i = \lambda_i - d$  for  $i \leq k$  and  $\lambda''_i = \lambda_{k+i}$  for  $i \leq n - k$ . Therefore, by (2.7) on one hand

$$(2.11) \quad s_{\lambda'}(1^k) = \prod_{i < j \leq k} \frac{\lambda'_i - \lambda'_j + j - i}{j - i} = \prod_{i < j \leq k} \frac{\lambda_i - \lambda_j + j - i}{j - i},$$

and on the other hand

$$s_{\lambda''}(1^{n-k}) = \prod_{i < j \leq n-k} \frac{\lambda''_i - \lambda''_j + j - i}{j - i} = \prod_{i < j \leq n-k} \frac{\lambda_{k+i} - \lambda_{k+j} + k + j - k + i}{k + j - k + i}$$

or equivalently

$$(2.12) \quad s_{\lambda''}(1^{n-k}) = \prod_{k < i < j \leq n} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

Dividing the product of (2.11) and (2.12) by  $s_\lambda(1^n)$  as given by (2.7), we obtain our claim (ii).

(iii) If  $\lambda_k < d$ , then  $[d]^k \subset \lambda$  is impossible, and if  $d < \lambda_{n-k+1}$  the  $(d+1)$ -th column of  $\lambda$  has length  $\geq n - k + 1$  and hence cannot be filled strictly increasingly by  $(1, \dots, n - k)$ , so that  $s_{\lambda \setminus [d]^k}(1^{n-k}) = 0$ . Thus  $\widehat{\mu_{k,n}}(\pi_m) = 0$  by (2.9).  $\square$

**Lemma 2.8.** *With the same notation as in Lemma 2.6:*

(i) *If  $d = 0$  then*

$$(2.13) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k+1)}{n(n+1)} \text{ if } \lambda_1 \geq 2.$$

$$(2.14) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k-1)}{n(n-1)} \text{ if } \lambda_1 = 1 \text{ and } \lambda \neq \lambda_+.$$

(ii) *If  $d \geq 1$  and  $n - k \leq k$  then*

$$(2.15) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k+1)}{n(n+1)} \text{ if } \lambda_k \geq 2.$$

$$(2.16) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k-1)}{n(n-1)} \text{ if } \lambda_k = \lambda_1 = 1 \text{ but } \lambda \neq \lambda_-.$$

$$(2.17) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k-1)}{n(n-1)} \text{ if } n-1 > k, \lambda_k = 1, \lambda_1 \geq 2 \text{ and } \lambda_{n-1} = 0.$$

$$(2.18) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{k(n-k)}{(n+1)(n-1)} \text{ if } \lambda_k = 1, \lambda_1 \geq 2 \text{ and } \lambda_{n-1} \geq 1.$$

*Proof.* (i) We will use Lemma 2.7 (i). Note that if  $\lambda_i \geq \mu_i \geq 0$  for all  $i \leq n$  we must have

$$\left( \prod_{i < j, j > n-k} \frac{\lambda_i + j - i}{j - i} \right)^{-1} \leq \left( \prod_{i < j, j > n-k} \frac{\mu_i + j - i}{j - i} \right)^{-1}.$$

Assume first that  $\lambda_1 \geq 2$ . We compare  $\lambda$  with  $\mu = (2, 0, \dots, 0)$ . Then

$$\prod_{i < j, j > n-k} \frac{\mu_i + j - i}{j - i} \geq \prod_{j > n-k} \frac{\mu_1 + j - 1}{j - 1} = \frac{n(n+1)}{(n-k)(n-k+1)}.$$

Now assume  $\lambda_1 = 1$ . Then  $\lambda = (1, \dots, 1, 0, 0, \dots)$  where 1 appears  $r$ -times.

If  $\lambda \neq \lambda_+$  (see Remark 2.4) we must have  $r \geq 2$ . Then comparing  $\lambda$  with  $\mu = (1, 1, 0, \dots, 0)$ , we obtain

$$\prod_{i < j, j > n-k} \frac{\lambda_i + j - i}{j - i} \geq \prod_{j > n-k} \frac{\mu_1 + j - 1}{j - 1} \prod_{j > n-k} \frac{\mu_2 + j - 2}{j - 2} = \frac{n}{n-k} \frac{n-1}{n-k-1}.$$

This proves (i).

We now turn to (ii). Assume  $d \geq 1$ . We use Lemma 2.7 (ii) but we distinguish several subcases:

† Assume first that  $\lambda_k \geq 2$ . Then, since  $\lambda_n = 0$

$$\prod_{i \leq k} \frac{\lambda_i - \lambda_n + n - i}{n - i} \geq \prod_{i \leq k} \frac{2 + n - i}{n - i} = \frac{n(n+1)}{(n-k)(n-k+1)}.$$

This proves (2.15).

†† Now assume  $\lambda_k = 1$ , so that  $d = 1$ . Then the case  $\lambda_1 = 1$  is easy. Indeed, let  $k \leq s < n$  be such that  $\lambda_j = 1$  for  $j \leq s$  and  $\lambda_j = 0$  for  $j > s$ . Since we exclude  $\lambda_-$ , we know that  $s < n-1$  (see Remark 2.4), and hence  $\lambda_{n-1} = 0$ . When  $n = 2$  this is impossible. When  $n = 3$ , the only possibility is  $k = 1$  and then  $\lambda \setminus [1]^k = 0$ , and hence  $\widehat{\mu_{k,n}}(\pi_m) = 0$ . Therefore, we may restrict to  $n \geq 4$ . Note  $s < n-1$  guarantees  $k < n-1$ . Then using both  $j = n$  and  $j = n-1$  we find

$$\begin{aligned} \prod_{i \leq k < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} &\geq \prod_{i \leq k} \frac{\lambda_i + n - i}{n - i} \prod_{i \leq k} \frac{\lambda_i + n - 1 - i}{n - 1 - i} \geq \prod_{i \leq k} \frac{1 + n - i}{n - i} \prod_{i \leq k} \frac{n - i}{n - 1 - i} \\ &= \frac{n(n-1)}{(n-k)(n-k-1)}. \end{aligned}$$

This proves (2.16).

††† Now assume  $\lambda_k = 1$  (and hence  $d = 1$ ) and  $\lambda_1 \geq 2$ .

**Case 1.** Assume first that  $\lambda_{n-1} = 0$ . Then, assuming  $n-1 > k$

$$\prod_{i \leq k < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \geq \prod_{i \leq k, j \in \{n, n-1\}} \frac{\lambda_i - \lambda_j + j - i}{j - i} \geq \prod_{i \leq k} \frac{\lambda_i + n - i}{n - i} \prod_{i \leq k} \frac{\lambda_i + n - 1 - i}{n - 2}$$

$$\geq \prod_{i \leq k} \frac{1+n-i}{n-i} \prod_{i \leq k} \frac{1+n-1-i}{n-1-i} = \frac{n}{n-k} \frac{n-1}{n-k-1}.$$

**Case 2.** Now assume  $\lambda_{n-1} \geq 1$ . Since we still assume  $\lambda_k = 1$  and  $\lambda_1 \geq 2$ , we can compare  $\lambda$  with  $\mu$  defined by  $\mu_1 = 2$ ,  $\mu_i = 1$  for all  $i < n$  and  $\mu_n = 0$ . Since  $\lambda \geq \mu$  and  $\mu_j = \lambda_j$  for all  $j > k$  we have

$$\prod_{i \leq k < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \geq \prod_{i \leq k < j} \frac{\mu_i - \mu_j + j - i}{j - i} = \prod_{k < j < n} \frac{\mu_1 - \mu_j + j - 1}{j - 1} \prod_{i \leq k} \frac{\mu_i - \mu_n + n - i}{n - i}$$

but

$$\prod_{k < j < n} \frac{\mu_1 - \mu_j + j - 1}{j - 1} = \frac{n-1}{k} \text{ and } \prod_{i \leq k} \frac{\mu_i - \mu_n + n - i}{n - i} = \frac{n+1}{n-1} \prod_{1 < i \leq k} \frac{n-i+1}{n-i} = \frac{n+1}{n-k}$$

and hence

$$\prod_{i \leq k < j} \frac{\mu_i - \mu_j + j - i}{j - i} \geq \frac{(n-1)(n+1)}{k(n-k)}.$$

This proves (2.17).  $\square$

*Remark 2.9.* In the proof of part (ii) in the preceding Lemma 2.8 the majorizations of  $\widehat{\mu_{k,n}}(\pi_m)$  appearing there are all proved actually for  $\left(\prod_{i \leq k < j} \frac{\lambda_i - \lambda_j + j - i}{j - i}\right)^{-1}$ .

**Lemma 2.10.** *With the same notation as in Lemma 2.6, let  $n > 3$  be an odd integer and let  $k = (n-1)/2 > 1$  so that  $n = 2k+1$ . If  $d \geq 1$  then*

$$(2.19) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k)(n-k-1)}{n(n+1)} \text{ if } \lambda_k \geq 2.$$

$$(2.20) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k-1)(n-k-2)}{n(n-1)} \text{ if } \lambda_k = 1 \text{ and } \lambda_1 = 1 \text{ but } \lambda \neq \lambda_-.$$

$$(2.21) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(n-k-1)(n-k-2)}{n(n-1)} \text{ if } \lambda_k = 1, \lambda_1 \geq 2 \text{ and } \lambda_{n-1} = 0.$$

$$(2.22) \quad \widehat{\mu_{k,n}}(\pi_m) \leq \frac{(k+1)(n-k-1)}{(n+1)(n-1)} \text{ if } \lambda_k = 1, \lambda_1 \geq 2 \text{ and } \lambda_{n-1} \geq 1.$$

*Proof.* We again decompose  $\lambda$  into  $\lambda'$  and  $\lambda''$ , but we will modify the definition of  $\lambda'$ . Now  $\lambda'$  will have  $k+1$  rows. Its first  $k$  rows being as before the same as those of  $\lambda \setminus [d]^k$ , and the  $(k+1)$ -th row being like this: if  $\lambda_{k+1} < d$  we set  $\lambda'_{k+1} = 0$ , while if  $\lambda_{k+1} \geq d$  we set  $\lambda'_{k+1} = \lambda_{k+1} - d$ . As for  $\lambda''$  it is formed as before of the last  $n-k$  rows of  $\lambda$ . Then arguing as in Lemma 2.6 we find

$$s_{\lambda \setminus [d]^k}(1^{n-k}) \leq s_{\lambda'}(1^{k+1}) s_{\lambda''}(1^{n-k}).$$

By (2.9) we have

$$\widehat{\mu_{k,n}}(\pi_m) \leq \frac{s_{\lambda'}(1^{k+1}) s_{\lambda''}(1^{n-k})}{s_{\lambda}(1^n)}.$$



We now use (2.7) for  $\lambda'$ ,  $\lambda''$  and  $\lambda$ . This gives us

$$\widehat{\mu_{k,n}}(\pi_m) \leq \left( \prod_{i \leq k+1 < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \right)^{-1} \prod_{i \leq k} \frac{\lambda'_i - \lambda'_{k+1} + k + 1 - i}{\lambda_i - \lambda_{k+1} + k + 1 - i}.$$

Now if  $\lambda_{k+1} \geq d$  the second factor is  $= 1$  and if  $\lambda_{k+1} < d$  we have  $\lambda'_i - \lambda'_{k+1} = \lambda_i - d < \lambda_i - \lambda_{k+1}$ . Thus we may remove that second factor. Therefore

$$\widehat{\mu_{k,n}}(\pi_m) \leq \left( \prod_{i \leq k+1 < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \right)^{-1}.$$

Thus it suffices to majorize  $\left( \prod_{i \leq k+1 < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \right)^{-1}$  by the bounds appearing in Lemma 2.10. We now invoke Remark 2.9. Observing that  $n - (k+1) \leq k+1$  we may apply part (ii) of Lemma 2.8 with  $k+1$  taking the place of  $k$ . Then replacing  $k$  by  $k+1$  in the upper bounds appearing in part (ii) in Lemma 2.8 and using Remark 2.9 we obtain the desired bounds for  $\left( \prod_{i \leq k+1 < j} \frac{\lambda_i - \lambda_j + j - i}{j - i} \right)^{-1}$ .  $\square$

*Proof of Theorem 2.1.* We apply first part (i) in Lemma 2.8 to settle the case  $d = 0$ . Thus we may assume  $d \geq 1$ . We apply then part (ii) from that same Lemma 2.8 to settle the cases either  $n = 2k$  or  $n = 2k - 1$ , with the restriction  $n - 1 > k$  which requires  $n > 3$ . Then Lemma 2.10 settles the remaining case  $n = 2k + 1$ . Note that  $k/n \rightarrow 1/2$  when  $n \rightarrow \infty$  if either  $k = n/2$ ,  $k = k_+$  or  $k = k_-$ , and all the bounds appearing in Lemmas 2.8 and 2.10 tend to  $1/4$ . Therefore, for any  $1/4 < \gamma < 1/2$  there is  $n(\gamma)$  such that for any  $n \geq n(\gamma)$

$$\sup_{\pi \notin S_n} \|\widehat{\nu_n}(\pi)\| \leq \gamma.$$

Since  $\widehat{\mu_{k,n}}(\pi) = k/n$  when  $\pi = \sigma_n$  or  $\pi = \overline{\sigma_n}$  (and since  $(k_+ + k_-)/2n = 1/2$ ) we have  $\widehat{\nu_n}(\pi) = 1/2$ . Thus  $\nu_n$  has a  $(1/2, \gamma)$ -spectral gap for any  $n \geq n(\gamma)$ , which settles the last assertion in Theorem 2.1. Checking the bounds for small values of  $n$ , actually we can find a  $\gamma < 1/2$  whenever  $n \geq 4$ .  $\square$

*Remark 2.11* (A natural question). Assume that  $k = [\theta n]$  where  $0 < \theta < 1$  is fixed. Then  $\widehat{\mu_{k,n}}(\sigma_n) = \widehat{\mu_{k,n}}(\overline{\sigma_n}) = (n - k)/n \approx 1 - \theta$ . By Lemmas 2.8 and 2.10, if we assume  $\theta \leq 1/2$  (to ensure that  $k \leq n - k$ ) then  $\mu_{k,n}$  has a  $(\delta_n, \gamma_n)$ -spectral gap with  $\delta_n \approx 1 - \theta$  and  $\gamma_n \approx (1 - \theta)^2$  when  $n \rightarrow \infty$ . We do not know whether this (or any similar spectral gap) holds when  $1/2 < \theta < 1$ .

### 3. Rider's results on Sidon sets

We now turn to the applications of the spectral gap obtained in Corollary 2.3 to Sidon sets. We start with two simple Lemmas. Their proof is not too different from their commutative version.

**Lemma 3.1.** *Let  $G$  be any compact group. Let  $\Lambda \subset \widehat{G}$  be randomly Sidon with constant  $C$ . Then for any finitely supported family  $(b_\pi)$  with  $b_\pi \in C(G; M_{d_\pi})$  ( $\pi \in \Lambda$ ) we have*

$$(3.1) \quad \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr} \left( \int \pi(g) b_\pi(g) m_G(dg) \right) \right| \leq C \int \left\| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi b_\pi) \right\|_\infty m_G(du).$$

*Proof.* Let  $f_\pi(t) = \int \pi(g)b_\pi(t^{-1}g)m_G(dg)$ . Then by the translation invariance of  $m_G$ ,  $t \mapsto \pi(t^{-1})f_\pi(t)$  is constant. Let

$$a_\pi = f_\pi(1) = \int \pi(g)b_\pi(g)m_G(dg).$$

Thus  $f_\pi(t) = \pi(t)f_\pi(1) = \pi(t)a_\pi$ . Let us write for short  $\mathbb{E}$  for the integral with respect to  $m_G$ . For any fixed  $g \in G$ , by translation invariance of the norm in  $C(G)$  and since  $(u_\pi)$  and  $(u_\pi\pi(g))$  have the same distribution, we have

$$\mathbb{E} \sup_{t \in G} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi b_\pi(t)) \right| = \mathbb{E} \sup_{t \in G} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi \pi(g) b_\pi(t^{-1}g)) \right|,$$

and hence

$$= \int \mathbb{E} \sup_{t \in G} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi \pi(g) b_\pi(t^{-1}g)) \right| m_G(dg)$$

and by Jensen this is

$$\geq \mathbb{E} \sup_{t \in G} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi f_\pi(t)) \right| = \mathbb{E} \sup_{t \in G} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi \pi(t) a_\pi) \right|.$$

Since  $\Lambda$  is assumed randomly Sidon, this last term is

$$\geq C^{-1} \sum_{\pi \in \Lambda} d_\pi \operatorname{tr} |a_\pi| \geq C^{-1} \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(a_\pi) \right|.$$

This completes the proof.  $\square$

*Remark 3.2.* Let  $b_\pi(g) = \pi(g^{-1})a_\pi$ . In that case (3.1) implies

$$\left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(a_\pi) \right| \leq C \int \left\| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(u_\pi \pi a_\pi) \right\|_\infty m_G(du).$$

This shows that (3.1) generalizes the randomly Sidon property.

**Lemma 3.3.** (i) Let  $\Lambda \subset \widehat{G}$  be a Sidon set with constant  $C$ . For any  $u \in \mathcal{G}$  (or merely for any  $u \in \prod_{\pi \in \Lambda} U(d_\pi)$ ) there is  $\mu^u \in M(G)$  with  $\|\mu^u\| \leq C$  such that  $\widehat{\mu^u}(\pi) = u_\pi$  for any  $\pi \in \Lambda$ .

(ii) Let  $\Lambda \subset \widehat{G}$  be a randomly Sidon set with constant  $C$ . Then, there is a functional  $\varphi \in L_1(\mathcal{G}; C(G))^*$  with norm  $\leq C$  such that for any  $\pi \in \Lambda$  and any  $b_\pi \in C(G; M_{d_\pi})$

$$\varphi(\operatorname{tr}(u_\pi b_\pi)) = \int \operatorname{tr}(\pi(g)b_\pi(g))m_G(dg).$$

(iii) Assuming (ii) and assuming  $C(G)$  separable, there is a weak\* measurable (in the sense of the following remark) bounded function  $u \mapsto \mu^u \in M(G)$  with  $\sup \|\mu^u\|_{M(G)} \leq C$  such that for any  $\pi \in \Lambda$

$$\mathbb{E}(u_\pi \mu^u) = \pi m_G.$$

The latter is an equality between matrix valued measures (or matrices with entries in  $M(G)$ ) by which we mean that for any  $f \in C(G)$  we have

$$\mathbb{E} \left( u_\pi \int f(g) \mu^u(dg) \right) = \int f(g) \pi(g) m_G(dg) = \widehat{f}(\bar{\pi}).$$

*Proof.* Both (i) and (ii) are immediate consequences of Hahn-Banach: For (i) we use the definition of Sidon sets and for (ii) we use Lemma 3.1. To check (iii), as explained in the next remark, we note that  $\varphi \in L_1(\mathcal{G}; C(G))^*$  defines a  $\mu^u$  such that  $\varphi(f(u)h(g)) = \mathbb{E}(f(u) \int h(g)\mu^u(dg))$  (here  $f \in L_1(\mathcal{G})$ ,  $h \in C(G)$ ), with  $\text{ess sup } \|\mu^u\|_{M(G)} = \|\varphi\|$ . Then (ii) can be rephrased as saying that the action of the  $d_\pi \times d_\pi$ -matrix (with entries in  $M(G)$ )  $\mathbb{E}(u_\pi \mu^u)$  on an arbitrary  $b_\pi \in C(G; M_{d_\pi})$  coincides with that of  $\pi(g)m_G$ . Then (iii) becomes clear.  $\square$

*Remark 3.4* (On the dual of  $L_1(\mathcal{G}; C(G))$ ). In the present paragraph  $(\mathcal{G}, m_G)$  can be any probability space. It is a well known fact that  $L_1(\mathcal{G}; C(G))$  is the projective tensor product of  $L_1(\mathcal{G})$  and  $C(G)$ , so that its dual can be identified isometrically to the space  $B(C(G), L_\infty(\mathcal{G}))$  of bounded linear maps from  $C(G)$  to  $L_\infty(\mathcal{G})$ . Explicitly, to any linear form  $\varphi \in L_1(\mathcal{G}; C(G))^*$  we naturally associate a bounded linear map  $T_\varphi : C(G) \rightarrow L_\infty(\mathcal{G})$  with  $\|T_\varphi\| = \|\varphi\|$  such that  $\varphi(f \otimes x) = \int (T_\varphi(f))(\omega)x(\omega)m_G(d\omega)$  for any  $f \in C(G)$ ,  $x \in L_1(\mathcal{G})$ .

Assume  $C(G)$  separable. Then  $\widehat{G}$  is countable and  $L_1(\mathcal{G})$  is also separable. Let  $D$  be a dense countable subset of  $C(G)$ , and let  $V$  be its linear span. Then any  $\xi \in C(G)^*$  is determined by its values on  $D$ , and also (by linearity) by its values on  $V$ . Clearly we can find a measurable subset  $\Omega_0 \subset \mathcal{G}$  with full measure on which all the maps  $\omega \mapsto |(T_\varphi(f))(\omega)|$  are bounded by  $\|T_\varphi\| \|f\|$  for any  $f \in D$ , and such that  $f \mapsto T_\varphi(f)(\omega)$  extends to a linear form of norm  $\leq \|T_\varphi\|$  on  $C(G)$  (for this one way is to consider linearity over the rationals). This allows us to define on  $\Omega_0$  a function  $\omega \mapsto \mu^\omega \in M(G)$  bounded by  $\|T_\varphi\|$  such that  $\omega \mapsto \mu^\omega(f) = \int f(g)\mu^\omega(dg)$  is measurable for any  $f \in D$  and hence for any  $f \in C(G)$  (this is what we mean by “weak\* measurability”) with  $\sup_{\Omega_0} \|\mu^\omega\| \leq \|T_\varphi\|$ , that represents  $\varphi$  in the sense that for a.a.  $\omega$

$$(3.2) \quad \int f(g)\mu^\omega(dg) = (T_\varphi(f))(\omega).$$

We denote by  $\mathcal{L}_\infty(\mathcal{G}; M(G))$  the space of all equivalence classes (modulo equality a.e.) of bounded weak\* measurable functions  $\omega \mapsto \mu^\omega \in M(G)$  equipped with the norm  $\text{ess sup}_\omega \|\mu^\omega\|$ . Conversely, for any such  $\omega \mapsto \mu^\omega \in M(G)$  we can associate a bounded linear map  $T : C(G) \rightarrow L_\infty(\mathcal{G})$  with  $\|T\| \leq \text{ess sup}_\omega \|\mu^\omega\|$  that takes  $f \in C(G)$  to the function  $\omega \mapsto \int f(g)\mu^\omega(dg)$ . Thus we obtain an isometric isomorphism between  $B(C(G), L_\infty(\mathcal{G}))$  and  $\mathcal{L}_\infty(\mathcal{G}; M(G))$ .

The preceding discussion shows that  $\mathcal{L}_\infty(\mathcal{G}; M(G))$  can be identified isometrically to the space  $L_1(\mathcal{G}; C(G))^*$ .

We now deduce Rider’s version of Drury’s Theorem :

**Theorem 3.5.** *Let  $G$  be any compact group. Let  $\Lambda \subset \widehat{G}$  be a randomly Sidon set with constant  $C$ . For any  $0 < \varepsilon < 1$  there is a measure  $\mu_\varepsilon \in M(G)$  such that*

$$(3.3) \quad \sup_{\pi \in \Lambda} \|\widehat{\mu}_\varepsilon(\pi) - I\| \leq \varepsilon \quad \forall \pi \in \Lambda, \quad \sup_{\pi \notin \Lambda} \|\widehat{\mu}_\varepsilon(\pi)\| \leq \varepsilon \quad \text{and} \quad \|\mu_\varepsilon\| \leq w(\varepsilon)$$

where  $w(\varepsilon)$  depends only on  $\varepsilon$  and  $C$ .

More generally, for any  $z \in \mathcal{G}$  (or merely for any  $z \in \prod_{\pi \in \Lambda} U(d_\pi)$ ), there is  $\mu_\varepsilon^z \in M(G)$  such that

$$\sup_{\pi \in \Lambda} \|\widehat{\mu}_\varepsilon^z(\pi) - z_\pi\| \leq \varepsilon \quad \forall \pi \in \Lambda, \quad \sup_{\pi \notin \Lambda} \|\widehat{\mu}_\varepsilon^z(\pi)\| \leq \varepsilon \quad \text{and} \quad \|\mu_\varepsilon^z\| \leq w(\varepsilon).$$

*Proof.* We have all the ingredients to reproduce the Drury-Rider trick. To avoid all irrelevant convergence and/or measurability issues, we assume that  $\Lambda$  is finite and that  $C(G)$  is separable. It is easy to pass from the finite case to the general one by a simple compactness argument (in the unit ball of  $M(G)$  equipped with the weak\* topology). Let  $\mu^u$  be as in Lemma 3.3 (iii). Let  $\Lambda' \subset \widehat{G}$

be the set formed by the coordinates  $\{u_\pi \mid \pi \in \Lambda\}$ . Note that here we abuse the notation: we still denote simply by  $u_\pi$  the irreducible representation  $u \mapsto u_\pi$  on  $\mathcal{G}$ .

By Corollary 2.3 there is  $\nu \in M(\mathcal{G})$  with  $\|\nu\| \leq w(\varepsilon)$  such that  $\widehat{\nu}(u_\pi) = \int \overline{u_\pi} \nu(du) = I$  for  $\pi \in \Lambda$  and  $\|\widehat{\nu}(r)\| = \|\int \overline{r}(u) \nu(du)\| \leq \varepsilon$  for any representation  $r \notin \Lambda'$ . Let

$$\Phi^u = \int \mu^{uu'} * \mu^{u'^{-1}} m_{\mathcal{G}}(du') \in \mathcal{L}_\infty(\mathcal{G}; M(G)).$$

Denoting  $\bar{z} = (\overline{z_\pi}) \in \mathcal{G}$ , we then define

$$\mu_\varepsilon^z = \int \Phi^{\bar{z}u} \nu(du).$$

Note

$$\|\mu_\varepsilon^z\| \leq C^2 w(\varepsilon).$$

A simple verification (using  $(\pi m_G) * (\pi m_G) = \pi m_G$ ) shows that (iii) in Lemma 3.3 is preserved, i.e. we have

$$\mathbb{E}(u_\pi \Phi^u) = \pi m_G,$$

and hence for each fixed  $z \in \mathcal{G}$

$$\overline{z_\pi} \mathbb{E}(u_\pi \Phi^{\bar{z}u}) = \mathbb{E}((\bar{z}u)_\pi \Phi^{\bar{z}u}) = \pi m_G.$$

Therefore

$$\mathbb{E}(u_\pi \Phi^{\bar{z}u}) = {}^t z_\pi \pi m_G.$$

More explicitly, for any fixed  $f \in C(G)$  if we denote  $\varphi_f(u) = \int f(g) \Phi^u(dg)$  we have

$$(3.4) \quad \forall \pi \in \Lambda \quad \mathbb{E}(u_\pi \varphi_f(\bar{z}u)) = {}^t z_\pi \widehat{f}(\bar{\pi}),$$

and hence taking the trace of both sides

$$(3.5) \quad \forall \pi \in \Lambda \quad \mathbb{E}(\text{tr}(u_\pi) \varphi_f(\bar{z}u)) = \text{tr}({}^t z_\pi \widehat{f}(\bar{\pi})).$$

By definition of  $\mu_\varepsilon^z$

$$(3.6) \quad \int f d\mu_\varepsilon^z = \int \varphi_f(\bar{z}u) \nu(du).$$

More generally, we can extend the definition of  $\varphi_f$  to any matrix-valued  $f \in C(G; M_d)$ : we simply set again

$$\varphi_f(u) = \int f(g) \Phi^u(dg).$$

Let  $\rho \in \widehat{G}$ . Note that  $\varphi_{\bar{\rho}} = \widehat{\Phi^u}(\rho)$ . Since  $\widehat{\Phi^u}(\rho) = \int \widehat{\mu^{uu'}}(\rho) \widehat{\mu^{u'^{-1}}}(\rho) m_{\mathcal{G}}(du')$  and  $\text{ess sup}_u \|\mu^u\| \leq C$ , the matrix valued function  $u \mapsto \varphi_\rho(u) = \widehat{\Phi^u}(\rho)$  (being the convolution on  $\mathcal{G}$  of two  $M_{d_\rho}$ -valued functions bounded by  $C$ ) has its coefficients in the space of absolutely convergent Fourier series  $A(\mathcal{G})$ , so that we can apply (1.10) (with  $\mathcal{G}$  in place of  $G$ ) to it.

Consider the “pseudo-measure”  $\nu'$  on  $\mathcal{G}$  defined a priori by its formal Fourier expansion

$$\nu' = \sum_{r \notin \Lambda'} d_r \text{tr}({}^t \widehat{\nu}(r) r).$$

Since we assume that  $\Lambda$  is finite  $\nu' \in M(G)$ , and since  $\widehat{\nu}(\pi) = I$  when  $\pi \in \Lambda$  we have

$$(3.7) \quad \nu = \left( \sum_{\pi \in \Lambda} d_\pi \text{tr}(u_\pi) \right) m_G + \nu'.$$

Recall that by our choice of  $\nu$  we have  $\sup_{r \in \widehat{G}} \|\widehat{\nu}'(r)\| \leq \varepsilon$ . By (1.10) we have for any  $\rho \in \widehat{G}$

$$(3.8) \quad \left\| \int \varphi_\rho(\bar{z}u) \nu'(du) \right\| \leq C^2 \sup_{r \in \widehat{G}} \|\widehat{\nu}'(r)\| \leq C^2 \varepsilon.$$

We claim that

$$\forall \pi \in \Lambda \quad \widehat{\mu}_\varepsilon^z(\pi) - z_\pi = \int \varphi_\pi(\bar{z}u) d\nu'(u)$$

and

$$\forall \rho \notin \Lambda \quad \widehat{\mu}_\varepsilon^z(\rho) = \int \varphi_\rho(\bar{z}u) d\nu'(u).$$

From this claim and (3.8) we obtain the conclusion, except that we obtain it with  $(C^2\varepsilon, C^2w(\varepsilon))$  in place of  $(\varepsilon, w(\varepsilon))$ .

Thus it only remains to justify the claim. By (3.6), (3.7) and (3.5) we have for any  $f \in C(G)$

$$(3.9) \quad \int f d\mu_\varepsilon^z - \int \varphi_f(\bar{z}u) d\nu'(u) = \int \varphi_f(\bar{z}u) \left( \sum_{\pi \in \Lambda} d_\pi \text{tr}(u_\pi) \right) dm_G(u) = \sum_{\pi \in \Lambda} d_\pi \text{tr}({}^t z_\pi \widehat{f}(\bar{\pi})).$$

Consider now the case  $f = \overline{\rho_{ij}}$ ,  $1 \leq i, j \leq d_\rho$ . We have  $\widehat{f}(\bar{\pi}) = 0$  if  $\rho \neq \pi$  and  $\widehat{f}(\bar{\pi}) = d_\pi^{-1} e_{ij}$  if  $\rho = \pi$ . Therefore we find

$$\sum_{\pi \in \Lambda} d_\pi \text{tr}({}^t z_\pi \widehat{f}(\bar{\pi})) = 1_{\rho \in \Lambda} (z_\pi)_{ij},$$

which by (3.9) implies our claim.  $\square$

**Corollary 3.6** (Rider, circa 1975, unpublished). *The union of two Sidon sets is a Sidon set.*

*Proof.* Let  $\Lambda \subset \widehat{G}$  be a Sidon set. In the situation of Theorem 3.5, for any  $f \in C(G)$  we have by the triangle inequality  $\|f * \mu_\varepsilon\|_\infty \geq \|\sum_{\pi \in \Lambda} d_\pi \text{tr}({}^t (\widehat{f * \mu_\varepsilon})(\pi) \pi)\|_\infty - \|\sum_{\pi \notin \Lambda} d_\pi \text{tr}({}^t (\widehat{f * \mu_\varepsilon})(\pi) \pi)\|_\infty$  and hence

$$w(\varepsilon) \|f\|_\infty \geq \|f * \mu_\varepsilon\|_\infty \geq ((1 - \varepsilon)/C) \sum_{\pi \in \Lambda} d_\pi \text{tr}|\widehat{f}(\pi)| - \varepsilon \|f\|_{A(G)}.$$

Let  $\Lambda_j \subset \widehat{G}$  be two disjoint Sidon sets with Sidon constants  $C_j$  ( $j = 1, 2$ ). Let  $f = f_1 + f_2 \in C(G)$  be a function with  $\widehat{f}_j$  supported in  $\Lambda_j$ . By the preceding inequality

$$w_1(\varepsilon) \|f\|_\infty \geq (1 - \varepsilon) C_1^{-1} \sum_{\pi \in \Lambda_1} d_\pi \text{tr}|\widehat{f}(\pi)| - \varepsilon \|f_2\|_{A(G)},$$

$$w_2(\varepsilon) \|f\|_\infty \geq (1 - \varepsilon) C_2^{-1} \sum_{\pi \in \Lambda_2} d_\pi \text{tr}|\widehat{f}(\pi)| - \varepsilon \|f_1\|_{A(G)},$$

and hence summing both

$$(w_1(\varepsilon) + w_2(\varepsilon)) \|f\|_\infty \geq ((1 - \varepsilon) \min\{C_1^{-1}, C_2^{-1}\} - \varepsilon) (\|f_1\|_{A(G)} + \|f_2\|_{A(G)}).$$

Then if we choose  $\varepsilon$  small enough so that  $C_\varepsilon = ((1 - \varepsilon) \min\{C_1^{-1}, C_2^{-1}\} - \varepsilon) > 0$  we find that  $\Lambda_1 \cup \Lambda_2$  is Sidon with constant at most  $(w_1(\varepsilon) + w_2(\varepsilon)) C_\varepsilon^{-1}$ .  $\square$

**Corollary 3.7** (Rider, circa 1975, unpublished). *Any randomly Sidon set is a Sidon set.*

*Proof.* In the situation of Theorem 3.5, for any  $z = (z_\pi) \in \mathcal{G}$  we have for any  $f \in C(G)$  with  $\widehat{f}$  supported in  $\Lambda$

$$w(\varepsilon)\|f\|_\infty \geq \|f * \mu_\varepsilon^z\|_\infty \geq \left| \sum_{\pi \in \Lambda} d_\pi \operatorname{tr}(\widehat{f}(\pi) z_\pi) \right| - \varepsilon \|f\|_{A(G)}$$

and hence taking the sup over  $z$

$$w(\varepsilon)\|f\|_\infty \geq (1 - \varepsilon)\|f\|_{A(G)}.$$

Thus, for any  $\varepsilon < 1$ ,  $\Lambda$  is Sidon with constant at most  $(1 - \varepsilon)^{-1}w(\varepsilon)$ .  $\square$

*Remark 3.8.* Actually, Corollary 3.7 implies Corollary 3.6, because it is easy to see that randomly Sidon sets are stable under finite unions.

*Remark 3.9.* Let  $\Lambda \subset \widehat{G}$  be Sidon with constant  $C$ . Assume that for all  $0 < \varepsilon < 1$  there is  $\mu_\varepsilon \in M(G)$  such that (3.3) holds. Then  $\Lambda$  is peaking. Indeed, by Hahn-Banach, for any  $z \in \prod_{\pi \in \Lambda} M_{d_\pi}$  with  $\sup_{\pi \in \Lambda} \|z_\pi\| < \infty$  there is  $\nu \in M(G)$  with  $\|\nu\|_{M(G)} \leq C \sup_{\pi \in \Lambda} \|z_\pi\|$  such that  $\widehat{\nu}(\pi) = z_\pi$  for any  $\pi \in \Lambda$ . Since  $\|\widehat{\mu}_\varepsilon(\pi) - I\| \leq \varepsilon < 1$ ,  $\widehat{\mu}_\varepsilon(\pi)$  is invertible and  $\|(\widehat{\mu}_\varepsilon(\pi))^{-1}\| \leq (1 - \varepsilon)^{-1}$  for any  $\pi \in \Lambda$ . Let  $z_\pi = (\widehat{\mu}_\varepsilon(\pi))^{-1}$ . Let  $\nu$  be the measure (given by Hahn-Banach) such that  $\|\nu\|_{M(G)} \leq C(1 - \varepsilon)^{-1}$  and  $\widehat{\nu}(\pi) = (\widehat{\mu}_\varepsilon(\pi))^{-1}$  for any  $\pi \in \Lambda$ . Let  $\nu_\varepsilon = \nu * \mu_\varepsilon$ . Then by (1.2)  $\widehat{\nu}_\varepsilon(\pi) = 1$  for  $\pi \in \Lambda$  and  $\|\widehat{\nu}_\varepsilon(\pi)\| \leq \|\nu\|_{M(G)} \|\widehat{\mu}_\varepsilon(\pi)\| \leq C\varepsilon(1 - \varepsilon)^{-1}$  for  $\pi \notin \Lambda$ . Also  $\|\nu_\varepsilon\|_{M(G)} \leq \|\nu\|_{M(G)} \|\mu_\varepsilon\|_{M(G)} \leq C(1 - \varepsilon)^{-1}w(\varepsilon)$ . This shows that  $\Lambda$  is an  $\varepsilon'$ -peak set for  $\varepsilon' = C\varepsilon(1 - \varepsilon)^{-1}$ . By Proposition 1.12 this shows that  $\Lambda$  is peaking.

*Remark 3.10.* In [63], Wilson managed to prove the union theorem in  $\widehat{G}$  when  $G$  is a *connected* compact group. His proof uses the structure theory of continuous compact groups and Lie groups. Apparently, it does not extend to general compact groups, and does not give any quantitative estimate.

## 4. Gaussian and Subgaussian random Fourier series

In this section we survey (with sketches of proofs) the main results of [37, 38]. We will take special care of Theorem 4.13 because unfortunately we detected a gap and probably an erroneous claim made by us in [38] concerning that statement (see Remark 4.14).

All the Gaussian variables we consider are always assumed (implicitly) to have mean 0. A Gaussian random variable  $g$  will be called normalized if  $\mathbb{E}|g|^2 = 1$ . We use this for either the real valued case or the complex valued one. We deliberately avoid the term “normal”, which usually implies that  $\mathbb{E}|g|^2 = 2$  in the complex case. By a complex valued Gaussian variable, we mean a variable of the form  $g = g_1 + ig_2$  such that  $g_1, g_2$  are independent (real valued) Gaussian variables with the same  $L_2$ -norm (and hence the same distribution).

Let  $(g_n)$  be an i.i.d. sequence of real (resp. complex) valued normalized Gaussian variables. Then for any nonzero real (resp. complex) sequence  $x = (x_n) \in \ell_2$ , the variable  $g = (\sum |x_n|^2)^{-1/2} \sum x_n g_n$  is a normalized Gaussian variable. Therefore

$$(4.1) \quad \left\| \sum x_n g_n \right\|_p = \|g_1\|_p \left( \sum |x_n|^2 \right)^{1/2}.$$

and also in the real (resp. complex) case

$$(4.2) \quad \mathbb{E} \exp\left(\sum x_n g_n\right) = \exp\left(\sum |x_n|^2/2\right) \quad (\text{resp. } \mathbb{E} \exp(\Re(\sum x_n g_n)) = \exp(\sum |x_n|^2/2)).$$

We now turn to the behaviour of Sidon sets in  $L_p$  for  $p < \infty$ . In many cases the growth of the  $L_p$ -norms of a function when  $p \rightarrow \infty$  is equivalent to its exponential integrability, as in the following elementary and well known Lemma.

We start by recalling the definition of certain Orlicz spaces. Let  $(\Omega, \mathbb{P})$  be a probability space. Let  $0 < a < \infty$ . Let

$$\forall x \geq 0 \quad \psi_a(x) = \exp x^a - 1.$$

We denote by  $L_{\psi_a}(\mathbb{P})$ , or simply by  $L_{\psi_a}$  the space of those  $f \in L_0(\Omega, \mathbb{P})$  for which there is  $t > 0$  such that  $\mathbb{E} \exp |f/t|^a < \infty$  and we set

$$\|f\|_{\psi_a} = \inf\{t > 0 \mid \mathbb{E} \exp |f/t|^a \leq e\}.$$

In the next two Lemmas (and Remark 4.2) we recall several well known properties of these spaces.

**Lemma 4.1.** *Fix a number  $a > 0$ . The following properties of a (real or complex) random variable  $f$  are equivalent:*

- (i)  $f \in L_p$  for all  $p < \infty$  and  $\sup_{p \geq 1} p^{-1/a} \|f\|_p < \infty$ .
- (ii)  $f \in L_{\psi_a}$ .
- (iii) There is  $t > 0$  such that  $\sup_{c > 0} \exp(tc^a) \mathbb{P}\{|f| > c\} < \infty$ .
- (iv) Let  $(f_n)$  be an i.i.d. sequence of copies of  $f$ . Then

$$\sup_n (\log(n+1))^{-1/a} |f_n| < \infty \text{ a.s. .}$$

Moreover, there is a positive constant  $C_a$  such that for any  $f \geq 0$  we have

$$(4.3) \quad C_a^{-1} \sup_{p \geq 1} p^{-1/a} \|f\|_p \leq \|f\|_{\psi_a} \leq C_a \sup_{p \geq 1} p^{-1/a} \|f\|_p,$$

and this still holds if we restrict the sup over  $p \geq 1$  to be over all even integers.

*Proof.* First observe that the conditions  $\sup_{p \geq 1} p^{-1/a} \|f\|_p < \infty$  and  $\sup_{p \geq a} p^{-1/a} \|f\|_p < \infty$  are obviously equivalent. Assume that  $\sup_{p \geq a} p^{-1/a} \|f\|_p \leq 1$ . Then

$$\mathbb{E} \exp |f/t|^a = 1 + \sum_1^\infty \mathbb{E} |f/t|^{an} (n!)^{-1} \leq 1 + \sum_1^\infty (an)^n t^{-an} (n!)^{-1}$$

hence by Stirling's formula for some constant  $C$

$$\leq 1 + C \sum_1^\infty (an)^n t^{-an} n^{-n} e^n = 1 + C \sum_1^\infty (at^{-a} e)^n$$

from which it becomes clear (since  $1 < e$ ) that (i) implies (ii). Conversely, if (ii) holds we have a fortiori for all  $n \geq 1$

$$(n!)^{-1} \|f/t\|_{an}^{an} \leq \mathbb{E} \exp |f/t|^a \leq e$$

and hence

$$\|f\|_{an} \leq e^{\frac{1}{an}} (n!)^{\frac{1}{an}} t \leq e^{\frac{1}{a}} n^{\frac{1}{a}} t = (an)^{\frac{1}{a}} t (e/a)^{1/a},$$

which gives  $\|f\|_p \leq p^{1/a} t (e/a)^{1/a}$  for the values  $p = an$ ,  $n = 1, 2, \dots$ . One can then easily interpolate (using Hölder's inequality) to obtain (i). The equivalences of (ii) with (iii) and (iv) are elementary exercises. The last assertion is a simple recapitulation left to the reader.  $\square$

*Remark 4.2.* Let

$$\|f\|_{\psi_a, \infty} = \inf\{t \mid \sup_{c>0}(\psi_a(c)\mathbb{P}(\{|f|/t\} > c)) \leq \psi_a(1)\}.$$

In addition to (ii)  $\Leftrightarrow$  (iii), it is easy to check that  $\|\cdot\|_{\psi_a, \infty}$  and  $\|\cdot\|_{\psi_a}$  are equivalent norms on  $L_{\psi_a}$ . This is in sharp contrast with the case of  $L_p$ -spaces (when we replace  $\psi_a$  by  $c \mapsto c^p$ ) for which weak- $L_p$  is a strictly larger space than  $L_p$ .

When  $\mathbb{E}f = 0$  (in the case  $a = 2$ ) the following variant explains why the variables such that  $\|f\|_{L_{\psi_2}} < \infty$  are usually called subGaussian. Indeed, by (4.2) if  $f$  is a normalized real valued Gaussian random variable, then the number  $sg(f)$  defined below is equal to 1 and equality holds in (4.4) when  $s=1$ . Although our terminology is slightly different, it is more customary to call subGaussian any variable satisfying (4.4) below.

**Lemma 4.3.** *If  $f$  is real valued, the following are equivalent:*

(i)  $f \in L_{\psi_2}$  and  $\mathbb{E}f = 0$ .

(ii) There is constant  $s \geq 0$  such that for any  $t \in \mathbb{R}$

$$(4.4) \quad \mathbb{E} \exp tf \leq \exp s^2 t^2 / 2.$$

Moreover, assuming  $\mathbb{E}f = 0$ ,  $\|f\|_{\psi_2}$  is equivalent to the number  $sg(f)$  defined as the smallest  $s \geq 0$  for which this holds.

*Proof.* Assume that  $f \in L_{\psi_2}$  with  $\|f\|_{\psi_2} \leq 1$ . Let  $f'$  be an independent copy of  $f$ . Let  $F = f - f'$ . Note that since the distribution of  $F$  is symmetric all its odd moments vanish, and hence

$$\mathbb{E} \exp xF = 1 + \sum_{n \geq 1} \frac{x^{2n}}{2n!} \mathbb{E} F^{2n}.$$

We have  $\|F\|_{\psi_2} \leq \|f\|_{\psi_2} + \|f'\|_{\psi_2} \leq 2$ . Therefore  $\mathbb{E}(F/2)^{2n} \leq n! \mathbb{E} \exp (F/2)^2 \leq en!$  and hence

$$\mathbb{E} \exp xF \leq 1 + \sum_{n \geq 1} \frac{(2x)^{2n}}{2n!} en! \leq 1 + \sum_{n \geq 1} \frac{(2\sqrt{e}x)^{2n}}{n!} \leq \exp(4ex^2).$$

But since  $t \mapsto \exp -xt$  is convex for any  $x \in \mathbb{R}$ , and  $\mathbb{E}f' = 0$  we have  $1 = e^0 \leq \mathbb{E} \exp -xf'$  and hence  $\mathbb{E} \exp xF = \mathbb{E} \exp xf \mathbb{E} \exp -xf' \geq \mathbb{E} \exp xf$ . Thus we conclude  $sg(f) \leq (8e)^{1/2}$ . By homogeneity this shows  $sg(f) \leq (8e)^{1/2} \|f\|_{\psi_2}$ .

Conversely, assume  $sg(f) \leq 1$ . Clearly (4.4) implies  $\mathbb{E}f = 0$ . Then for any  $x, t > 0$

$$\mathbb{P}(\{f > x\})e^{tx} \leq \mathbb{E}e^{tf} \leq e^{x^2/2}.$$

taking  $x = t$  we find  $\mathbb{P}(\{f > t\}) \leq e^{-t^2/2}$ , and since  $sg(-f) = sg(f) \leq 1$  we also have  $\mathbb{P}(\{-f > t\}) \leq e^{-t^2/2}$ , and hence

$$\mathbb{P}(\{|f| > t\}) \leq 2e^{-t^2/2}.$$

Fix  $c > \sqrt{2}$ . Let  $\theta = 1/2 - 1/c^2$ . Note  $\theta > 0$ .

$$\mathbb{E} \exp (f/c)^2 - 1 = \int_0^\infty (2t/c^2) \exp (t/c)^2 \mathbb{P}(\{|f| > t\}) dt \leq \int_0^\infty (4t/c^2) e^{-\theta t^2} dt = 2/\theta c^2.$$

Elementary calculation shows that if  $c_0 = (2(e+1)(e-1)^{-1})^{1/2}$  we have  $1 + 2/\theta c_0^2 = e$ . Thus we conclude  $\|f\|_{\psi_2} \leq c_0$ . By homogeneity, this shows  $\|f\|_{\psi_2} \leq c_0 sg(f)$ .  $\square$



The next result was repeatedly used in [34]. It shows that independent random unitary matrices are dominated in a strong sense by their Gaussian analogues.

**Lemma 4.4.** *Let  $(d_k)_{k \in I}$  be an arbitrary collection of integers. Let  $\mathbf{G} = \prod_{k \in I} U(d_k)$ . Let  $u \mapsto u_k$  denote the coordinates on  $\mathbf{G}$ , and  $u_k(i, j)$  ( $1 \leq i, j \leq d_k$ ) the entries of  $u_k$ . Let  $\{g_k(i, j)\}$  ( $1 \leq i, j \leq d_k$ ) be a collection of independent complex valued Gaussian random variables such that  $\mathbb{E}(g_k(i, j)) = 0$  and  $\mathbb{E}|g_k(i, j)|^2 = 1/d_k$ , on a probability space  $(\Omega, \mathbb{P})$ . For some  $C_0 > 0$  there is a positive operator  $T : L_1(\Omega, \mathbb{P}) \rightarrow L_1(\mathbf{G}, m_{\mathbf{G}})$  with  $\|T : L_p(\Omega, \mathbb{P}) \rightarrow L_p(\mathbf{G}, m_{\mathbf{G}})\| \leq C_0$  for all  $1 \leq p \leq \infty$  such that*

$$\forall k \forall i, j \leq d_k \quad T(g_k(i, j)) = u_k(i, j).$$

*Sketch.* Let  $g_k = v_k |g_k|$  be the polar decomposition of  $g_k$ . Let  $\mathcal{E}$  be the conditional expectation with respect to  $(v_k)$ . Since  $(v_k)$  and  $(|g_k|)$  are independent random variables, we have  $\mathcal{E}(g_k) = v_k \mathbb{E}|g_k|$ . By known results  $\mathbb{E}|g_k| = \delta_k I$  for some  $\delta_k > 0$  such that  $\delta = \inf_k \delta_k > 0$ . Thus  $\mathcal{E}(g_k) = v_k \delta_k$ . Since  $0 < \delta/\delta_k < 1$  for all  $k$ , it is easy to see there is a (positive) operator  $W : L_p(\mathbf{G}, m_{\mathbf{G}}) \rightarrow L_p(\mathbf{G}, m_{\mathbf{G}})$  with  $\|W\| \leq 1$  for any  $1 \leq p \leq \infty$ , such that  $W(v_k) = (\delta/\delta_k)v_k$  and hence  $\delta^{-1}W\mathcal{E}(g_k) = v_k$ . Thus, since  $(u_k)$  and  $(v_k)$  have the same distribution,  $T = \delta^{-1}W\mathcal{E}$  gives us the desired operator.  $\square$

*Remark 4.5* (Matricial contraction principle). Let  $(u_k)$  and  $(g_k)$  be as in Lemma 4.4. Let  $\{x_k(i, j) \mid k \geq 1, 1 \leq i, j \leq d_k\}$  be a finitely supported family in an arbitrary Banach space  $B$ . For any matrix  $a \in M_{d_k}$  with complex entries, we denote by  $ax$  and  $xa$  the matrix products (with entries in  $B$ ). By convention, we write  $\text{tr}(u_k x_k) = \sum_{ij} u_k(i, j)x_k(j, i)$ . With this notation, the following “contraction principle” holds

$$\int \left\| \sum d_k \text{tr}(a_k u_k b_k x_k) \right\| dm_{\mathbf{G}} \leq \sup_k \|a_k\|_{M_{d_k}} \sup_k \|b_k\|_{M_{d_k}} \int \left\| \sum d_k \text{tr}(u_k x_k) \right\| dm_{\mathbf{G}}.$$

Indeed, this is obvious by the translation invariance of  $m_{\mathbf{G}}$  if  $a_k, b_k$  are all unitary. Then the result follows since the unit ball of  $M_{d_k}$  is the closed convex hull of its extreme points, namely its unitary elements.

The same inequality holds if we replace  $(u_k)$  by any sequence of variables  $(z_k)$  such that for any unitary matrices  $a_k, b_k \in U(d_k)$  the sequences  $(z_k)$  and  $(a_k z_k b_k)$  have the same distribution. In particular this holds for the Gaussian sequence  $(g_k)$ .

**Notation:** Let  $G$  be any compact group. We denote by  $(g_{\pi})$  an independent family indexed by  $\widehat{G}$ , defined like this:  $g_{\pi}$  is a random  $d_{\pi} \times d_{\pi}$ -matrix the entries of which are independent complex Gaussian random variables with  $L_2$ -norm  $= (1/d_{\pi})^{1/2}$ . All our random variables are assumed defined on a suitable probability space  $(\Omega, \mathbb{P})$ .

In the sequel, we similarly think of  $(u_{\pi})$  as an independent family of unitary  $d_{\pi} \times d_{\pi}$ -matrices indexed by  $\widehat{G}$ , on the probability space  $(\mathcal{G}, m_{\mathcal{G}})$ . For simplicity we denote the integral on  $\mathcal{G}$  by  $\mathbb{E}$ .

The following basic fact compares the notions of randomly Sidon for  $(g_{\pi})$  and  $(u_{\pi})$ . It is proved by the same truncation trick that was used in [37]. See [34, Chap.V and VI] for further details and more general facts.

**Lemma 4.6.** *For a subset  $\Lambda \subset \widehat{G}$ , the following are equivalent:*

(i) *There is a constant  $\alpha_1$  such that for any finitely supported family  $(a_{\pi}) \in \prod_{\pi \in \Lambda} M_{d_{\pi}}$*

$$\sum_{\pi \in \Lambda} d_{\pi} \text{tr}|a_{\pi}| \leq \alpha_1 \mathbb{E} \left\| \sum_{\pi \in \Lambda} d_{\pi} \text{tr}(g_{\pi} \pi a_{\pi}) \right\|_{\infty}.$$

(ii) *There is a constant  $\alpha_2$  such that for any finitely supported family  $(a_{\pi}) \in \prod_{\pi \in \Lambda} M_{d_{\pi}}$*

$$\sum_{\pi \in \Lambda} d_{\pi} \text{tr}|a_{\pi}| \leq \alpha_2 \mathbb{E} \left\| \sum_{\pi \in \Lambda} d_{\pi} \text{tr}(u_{\pi} \pi a_{\pi}) \right\|_{\infty}.$$

*Sketch.* From Lemma 4.4 it is easy to deduce that

$$\mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} \pi a_{\pi}) \right\|_{\infty} m_{\mathbf{G}}(du) \leq C_0 \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(g_{\pi} \pi a_{\pi}) \right\|_{\infty},$$

and hence (ii)  $\Rightarrow$  (i). To check the converse, recall the well known fact that  $c_4 = \sup \mathbb{E} \|g_{\pi}\|^2 < \infty$ , from which it is easy to deduce by Chebyshev's inequality that there exists  $c_5 > 0$  such that

$$\sup \mathbb{E} (\|g_{\pi}\| 1_{\{\|g_{\pi}\| > c_5\}}) \leq (2\alpha_1)^{-1}.$$

We may assume that the sequences  $(u_{\pi})$  and  $(g_{\pi})$  are mutually independent, so that the sequences  $(g_{\pi})$  and  $(u_{\pi} g_{\pi})$  have the same distribution. Then by the triangle inequality and by Remark 4.5

$$\begin{aligned} \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(g_{\pi} \pi a_{\pi}) \right\|_{\infty} &= \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} g_{\pi} \pi a_{\pi}) \right\|_{\infty} \\ &\leq \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} g_{\pi} 1_{\{\|g_{\pi}\| \leq c_5\}} \pi a_{\pi}) \right\|_{\infty} + \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} g_{\pi} 1_{\{\|g_{\pi}\| > c_5\}} \pi a_{\pi}) \right\|_{\infty} \\ &\leq c_5 \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} \pi a_{\pi}) \right\|_{\infty} + \mathbb{E} \sum_{\Lambda} d_{\pi} \|g_{\pi}\| 1_{\{\|g_{\pi}\| > c_5\}} |\operatorname{tr} a_{\pi}| \\ &\leq c_5 \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} \pi a_{\pi}) \right\|_{\infty} + (2\alpha_1)^{-1} \sum_{\Lambda} d_{\pi} \operatorname{tr} |a_{\pi}|. \end{aligned}$$

Using this we see that (i) implies

$$\sum_{\Lambda} d_{\pi} \operatorname{tr} |a_{\pi}| \leq \alpha_1 c_5 \mathbb{E} \left\| \sum_{\Lambda} d_{\pi} \operatorname{tr}(u_{\pi} \pi a_{\pi}) \right\|_{\infty} + (1/2) \sum_{\Lambda} d_{\pi} \operatorname{tr} |a_{\pi}|,$$

and hence (i)  $\Rightarrow$  (ii) with  $\alpha_2 \leq 2\alpha_1 c_5$ .  $\square$

*Remark 4.7* (Comparison of randomizations). Actually, Lemma 4.6 follows from a much more general fact proved in [34]. Let  $(a_{\pi})$  be a finitely supported family indexed by  $\widehat{G}$  with  $a_{\pi} \in M_{d_{\pi}}$  ( $\pi \in \widehat{G}$ ). In [34], the random Fourier series

$$R(x) = \sum_{\pi \in \widehat{G}} d_{\pi} \operatorname{tr}(u_{\pi} \pi(x) a_{\pi}) \quad (x \in G)$$

randomized by  $u = (u_{\pi})$  on  $(\mathcal{G}, m_{\mathcal{G}})$  is compared to

$$\widetilde{R}(x) = \sum_{\pi \in \widehat{G}} d_{\pi} \operatorname{tr}(g_{\pi} \pi(x) a_{\pi}) \quad (x \in G)$$

randomized by  $g_{\pi}$  on  $(\Omega, \mathbb{P})$ . By [34, p.97] there is a universal constant  $c > 0$  such that

$$(4.5) \quad c^{-1} \mathbb{E} \sup_{x \in G} |\widetilde{R}(x)| \leq \mathbb{E} \sup_{x \in G} |R(x)| \leq c \mathbb{E} \sup_{x \in G} |\widetilde{R}(x)|.$$

In particular, a set is randomly Sidon iff it so when we replace the random unitaries  $(u_{\pi})$  by the Gaussian variables  $g_{\pi}$ , so we recover Lemma 4.6.

*Remark 4.8.* A similar comparison holds for the random Fourier series

$$L(x) = \sum d_{\pi} \operatorname{tr}(u_{\pi} a_{\pi} \pi(x)) \quad (x \in G) \text{ and } \widetilde{L}(x) = \sum d_{\pi} \operatorname{tr}(g_{\pi} a_{\pi} \pi(x)) \quad (x \in G),$$

where the randomization is on the other side of  $\pi$ , but this can be easily derived from the case of  $R$  and  $\widetilde{R}$  by observing that

$$|L(x)| = |\overline{L(x)}| = \left| \sum d_{\pi} \operatorname{tr}((u_{\pi} a_{\pi} \pi(x))^*) \right| = \left| \sum d_{\pi} \operatorname{tr}(u_{\pi}^* \pi(x^{-1}) a_{\pi}^*) \right|,$$

and the last series can be treated as  $R(x^{-1})$  for a suitable  $R$ .

*Remark 4.9.* By passing to the series  $\tilde{R}$ , we allow ourselves the use of the rich theory of Gaussian processes. We will use these ideas to prove the next statement. Let us briefly outline this. Let  $f(x) = \sum_{\pi \in \hat{G}} d_\pi \text{tr}(\pi(x) a_\pi)$  so that  ${}^t \hat{f}(\pi) = a_\pi$ . Let  $f_t(g) = f(gt)$ . Let

$$d_f(s, t) = \|\tilde{R}(s) - \tilde{R}(t)\|_2 = \|f_s - f_t\|_2 = \left( \sum d_\pi \text{tr} |(\pi(s) - \pi(t))^t \hat{f}(\pi)|^2 \right)^{1/2}.$$

The metric entropy integral associated to  $f$  is usually defined as

$$\int_0^\infty (\log N_f(\varepsilon))^{1/2} d\varepsilon$$

where  $N_f(\varepsilon)$  is the smallest number of open balls of  $d_f$ -radius  $\varepsilon$  that suffice to cover  $G$ . Since the measure and the distance are both (left) translation invariant, one checks easily that

$$(4.6) \quad m_G(\{t \mid d_f(t, 1) < \varepsilon\})^{-1} \leq N_f(\varepsilon) \leq m_G(\{t \mid d_f(t, 1) < \varepsilon/2\})^{-1}.$$

Thus we may work with the following quantity equivalent to the metric entropy integral :

$$\mathcal{I}_2(f) = \int_0^\infty \left( \log \frac{1}{m_G(\{t \mid d_f(t, 1) < \varepsilon\})} \right)^{1/2} d\varepsilon.$$

The metric entropy integral was originally introduced in the subject in a 1967 paper of Dudley to give new upper bounds for general Gaussian processes. In the stationary case, Fernique showed that the same integral is also a lower bound. The latter bound implies that there is an absolute constant  $c$  such that

$$(4.7) \quad \mathcal{I}_2(f) \leq c \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty.$$

A fortiori, this implies Sudakov's minoration (see e.g. [41, p.69] or [58]): there is a numerical constant  $c'$  such that

$$\sup_{\varepsilon > 0} \varepsilon (\log N_f(\varepsilon))^{1/2} \leq c' \mathbb{E} \sup_{x \in G} |\tilde{R}(x)|,$$

and hence

$$(4.8) \quad \sup_{\varepsilon > 0} \varepsilon \left( \log \frac{1}{m_G(\{x \mid d(x, 1) < \varepsilon\})} \right)^{1/2} \leq cc' \mathbb{E} \sup_{x \in G} |R(x)|.$$

The next two Theorems essentially come from [37, 38]. They show that a set is Sidon iff it is a  $\Lambda(p)$ -set (in Rudin's sense [51]) for all  $p > 2$  with a constant growing at most like  $\sqrt{p}$ .

**Theorem 4.10** (Sidon versus  $\Lambda(p)$ -sets). *Let  $\Lambda \subset \hat{G}$ . The following three assertions are equivalent:*

- (i)  $\Lambda$  is a Sidon set.
- (ii) There is a constant  $C$  such that for any  $f \in L_2(G)$  with  $\hat{f}$  supported in  $\Lambda$  we have

$$\|f\|_{\psi_2} \leq C \|f\|_2.$$

- (ii)' There is a constant  $C$  such that for any finitely supported family  $(a_\pi)$  ( $a_\pi \in M_{d_\pi}$ ) we have for any  $p \geq 2$

$$\left\| \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi a_\pi) \right\|_p \leq Cp^{1/2} \left( \sum_{\pi \in \Lambda} d_\pi \text{tr}|a_\pi|^2 \right)^{1/2}.$$

*Sketch.* The equivalence between (ii) and (ii)' is immediate by (4.3). The proof that (i)  $\Rightarrow$  (ii) follows a classical argument due to Rudin that Figà-Talamanca and Rider adapted to the non-Abelian case. The quicker argument in [34] avoids their moment computations by using instead Lemma 4.4, but first we use (i) in Lemma 3.3. With the notation in that Lemma, assuming  $\Lambda$  Sidon, the operator of convolution by  $\mu^u$  has norm  $\leq C$  on  $L_p(G)$  for any  $1 \leq p \leq \infty$ . Therefore, for any  $f = \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi^t \hat{f}(\pi))$  (finite sum) we have

$$\left\| \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi^t (u_\pi \hat{f}(\pi))) \right\|_p \leq C \|f\|_p.$$

As before let  $\mathcal{G} = \prod_{\pi \in \hat{G}} U(d_\pi)$  (actually we could work simply with  $\prod_{\pi \in \Lambda} U(d_\pi)$ ). Let  $u = (u_\pi) \in \mathcal{G}$ . Let  $F_u = \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi^t (u_\pi^* \hat{f}(\pi)))$ . Applying this with  $F_u$  in place of  $f$  we find

$$\|f\|_p \leq C \|F_u\|_p$$

and hence

$$\|f\|_p \leq C \left( \int \|F_u\|_p^p m_{\mathcal{G}}(du) \right)^{1/p}.$$

Note  $F_u = \sum_{\pi \in \Lambda} d_\pi \text{tr}(u_\pi^* \hat{f}(\pi)^t \pi)$ . By Lemma 4.4

$$\left( \int \|F_u\|_p^p m_{\mathcal{G}}(du) \right)^{1/p} \leq C_0 (\mathbb{E} \left\| \sum_{\pi \in \Lambda} d_\pi \text{tr}(g_\pi \hat{f}(\pi)^t \pi) \right\|_p^p)^{1/p}$$

and since  $({}^t \pi(x) g_\pi(\omega))$  (on  $G \times \Omega$ ) and  $(g_\pi)$  (on  $\Omega$ ) have the same distribution, we have using (4.1)

$$(\mathbb{E} \left\| \sum_{\pi \in \Lambda} d_\pi \text{tr}(g_\pi \hat{f}(\pi)^t \pi) \right\|_p^p)^{1/p} = (\mathbb{E} \left| \sum_{\pi \in \Lambda} d_\pi \text{tr}(g_\pi \hat{f}(\pi)) \right|_p^p)^{1/p} = \gamma(p) \|f\|_2$$

where  $\gamma(p)$  is the  $L_p$ -norm of a normalized complex Gaussian variable. This gives us

$$\|f\|_p \leq C C_0 \gamma(p) \|f\|_2,$$

and since  $\gamma(p) = O(\sqrt{p})$ , we obtain (ii) by (4.3).

The proof that (ii)  $\Rightarrow$  (i) in [37, 34] uses the metric entropy characterization of the Gaussian random Fourier series that are continuous a.s.. We merely outline the original argument. Fix  $f = \sum_{\pi \in \Lambda} d_\pi \text{tr}(\pi^t \hat{f}(\pi))$  (finite sum). We will use Gaussian process theory through the *minoration* (4.7). But, by another result from that theory (a variant of Dudley's upper bound), the integral  $\mathcal{I}_2(f)$  *majorizes* the subGaussian processes that are suitably dominated in the metric sense by  $d_f$ . More specifically, since (ii) implies  $\|f_s - f_t\|_{\psi_2} \leq C d_f(s, t)$  the said majorization implies (assuming  $\int f dm_G = 0$ ) that ( $c'$  is here an absolute constant)

$$(4.9) \quad \|f\|_\infty \leq c' C \mathcal{I}_2(f).$$

Therefore, we obtain

$$(4.10) \quad \|f\|_\infty \leq c' C \mathcal{I}_2(f) \leq c c' C \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty,$$

and hence

$$(4.11) \quad \left| \sum d_\pi \text{tr}({}^t \hat{f}(\pi)) \right| = |f(1)| \leq c c' C \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty.$$

But by the distributional invariance property of  $(g_\pi)$  we have for any  $z_\pi \in U(d_\pi)$

$$\mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty = \mathbb{E} \left\| \sum d_\pi \text{tr}(z_\pi g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty = \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi ({}^t \hat{f}(\pi) z_\pi)) \right\|_\infty,$$

and hence (4.11) applied to  $\sum d_\pi \text{tr}(g_\pi \pi(t \hat{f}(\pi) z_\pi))$  implies after taking the sup over  $z_\pi$

$$\sum_{\pi \in \Lambda} d_\pi \text{tr}(|\hat{f}(\pi)|) = \sum_{\pi \in \Lambda} d_\pi \text{tr}(|t \hat{f}(\pi)|) \leq cc' C \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty.$$

In other words, provided we can replace  $(g_\pi)$  by  $(u_\pi)$ , we conclude that  $\Lambda$  is randomly Sidon and hence Sidon by Corollary 3.7. The replacement of  $(g_\pi)$  by  $(u_\pi)$  is justified by Lemma 4.6 (see also the discussion around (4.5)).  $\square$

*Remark 4.11.* Let  $f \in C(G)$ . Note  $\|f\|_\infty = \int \sup_{x \in G} |f(tx)| m_G(dt)$ . For proper perspective, we use this observation to rewrite (4.10) as

$$(4.12) \quad \|f\|_\infty = \int \left\| \sum d_\pi \text{tr}(\pi(t) \pi^t \hat{f}(\pi)) \right\|_\infty m_G(dt) \leq cc' C \mathbb{E} \left\| \sum d_\pi \text{tr}(g_\pi \pi^t \hat{f}(\pi)) \right\|_\infty.$$

Let  $Y_x(t) = \sum d_\pi \text{tr}(\pi(t) \pi(x)^t \hat{f}(\pi))$  and  $X_x(\omega) = \sum d_\pi \text{tr}(g_\pi(\omega) \pi(x)^t \hat{f}(\pi))$ . Then (4.12) means

$$(4.13) \quad \int \sup_{x \in G} |Y_x| dm_G \leq cc' C \mathbb{E} \sup_{x \in G} |X_x|.$$

In the preceding proof the Dudley-Fernique metric entropy bounds were used only to prove (4.12) or equivalently (4.13). These require a certain group invariance (namely the process  $(X_x)$  must be a stationary Gaussian process). Inspired by the latter bounds, Talagrand [57] managed to prove a general version of (4.13) that does not require any group invariance. More precisely, he proved that there is an absolute constant  $\tau_0$  such that:

If  $(\varphi_n)$  are variables such that for any finitely supported scalar sequence  $(a_n)$  we have

$$\left\| \sum a_n \varphi_n \right\|_{\psi_2} \leq \left( \sum |x_n|^2 \right)^{1/2}$$

and if  $(f_n)$  are arbitrary functions on a set  $S$  then we have

$$\mathbb{E} \sup_{x \in S} \left| \sum \varphi_n f_n(x) \right| \leq \tau_0 \mathbb{E} \sup_{x \in S} \left| \sum g_n f_n(x) \right|.$$

We use this in our recent paper [44] to prove a version of the implication subGaussian  $\Rightarrow$  Sidon for general uniformly bounded orthonormal systems, that improves an earlier breakthrough due to Bourgain and Lewko [3]. We also give in [44] an analogue of (ii)  $\Rightarrow$  (i) in Theorem 4.10 to the case when the system  $\{d_\pi^{1/2} \pi_{ij} \mid \pi \in \Lambda, 1 \leq i, j \leq d_\pi\}$  is replaced by an orthonormal system on a probability space  $(T, m)$  indexed by a set  $\Lambda$  such that the norms of the  $d_\pi \times d_\pi$  matrices  $[\pi_{ij}(t)]$  are uniformly bounded over  $t \in T$  and  $\pi \in \Lambda$ . In the same framework, we also give an analogue of the equivalence between Sidon and randomly Sidon. See §6 for a related application of these ideas.

The following refinement of Theorem 4.10 proved in [38] will be useful.

**Lemma 4.12.** *Assume that  $G$  is Abelian (so that  $d_\pi = 1$  for all  $\pi$ ). Let  $1 < p < 2 < p' < \infty$  such that  $1/p + 1/p' = 1$ . Assume that there is a constant  $C$  such that for any  $f \in L_2(G)$  with  $\hat{f}$  supported in  $\Lambda$  we have*

$$(4.14) \quad \|f\|_{\psi_{p'}} \leq C \left( \sum_{\pi \in \Lambda} |\hat{f}(\pi)|^p \right)^{1/p}.$$

*Then  $\Lambda$  is Sidon.*

*Proof.* Let

$$d_{p,f}(t, s) = (\sum_{\pi \in \hat{G}} |\hat{f}(\pi)(\pi(t) - \pi(s))|^p)^{1/p}.$$

We will use a variant of the metric entropy integral  $\mathcal{I}_2(f)$ , namely

$$\mathcal{I}_p(f) = \int_0^\infty (\log \frac{1}{m_G(\{t \mid d_{p,f}(t, 1) < \varepsilon\})})^{1/p'} d\varepsilon.$$

Schematically, the proof can be described like this: By a generalization of the Dudley majorization (4.9) we have (assuming still  $\int f dm_G = 0$ ) that if we assume

$$\forall t, s \in G \quad \|f_t - f_s\|_{\psi_{p'}} \leq C d_{p,f}(t, s)$$

then we have

$$\|f\|_\infty \leq C c'_p \mathcal{I}_p(f),$$

and replacing  $f$  by  $\sum_{\pi \in \hat{G}} |\hat{f}(\pi)| \pi$  (which leaves  $d_{p,f}$  and hence also  $\mathcal{I}_p(f)$  invariant) we find

$$(4.15) \quad \sum_{\pi \in \hat{G}} |\hat{f}(\pi)| \leq C c'_p \mathcal{I}_p(f).$$

This shows that if  $\Lambda$  satisfies the assumption (4.14) then any  $f \in L_2(G)$  with  $\hat{f}$  supported in  $\Lambda \setminus \{0\}$  satisfies

$$(4.16) \quad \sum_{\pi \in \Lambda} |\hat{f}(\pi)| \leq C c'_p \mathcal{I}_p(f).$$

We may assume  $0 \notin \Lambda$  for simplicity. The conclusion will follow from the following inequality

$$(4.17) \quad \mathcal{I}_p(f) \leq c'' (\sum_{\pi \in \hat{G}} |\hat{f}(\pi)|)^{1-\theta} \mathcal{I}_2(f)^\theta,$$

where  $c''$  depends only on  $p$  and where  $0 < \theta < 1$ .

Indeed, (4.17) combined with (4.16) implies

$$\sum_{\pi \in \Lambda} |\hat{f}(\pi)| \leq C c'_p c'' (\sum_{\pi \in \hat{G}} |\hat{f}(\pi)|)^{1-\theta} \mathcal{I}_2(f)^\theta,$$

and after a suitable division we find

$$\sum_{\pi \in \Lambda} |\hat{f}(\pi)| \leq (C c'_p c'')^{1/\theta} \mathcal{I}_2(f).$$

But now using Fernique's lower bound (4.7), we conclude as in the preceding proof that  $\Lambda$  is Sidon. It remains to justify (4.17). Let  $N_p(\varepsilon)$  denote the smallest number of sets of  $d_{p,f}$ -diameter  $\leq \varepsilon$  that suffice to cover  $G$ . Let  $e_n(d_{p,f})$  be the smallest number  $\varepsilon$  such that  $G$  can be covered by  $2^n$  sets of  $d_{p,f}$ -diameter  $\leq \varepsilon$  (i.e. such that  $N_p(\varepsilon) \leq 2^n$ ). We first note that  $\mathcal{I}_p(f)$  is equivalent to

$$\int_0^\infty (\log N_p(\varepsilon))^{1/p'} d\varepsilon.$$

Then, since  $\int_0^\infty (\log N_p(\varepsilon))^{1/p'} d\varepsilon = \sum_n \int_{e_n}^{e_{n+1}} (\log N_p(\varepsilon))^{1/p'} d\varepsilon$  one checks easily that the latter quantity is equivalent to the following one:

$$\Sigma_p(f) = \sum_0^\infty e_n(d_{p,f}) n^{-1/p'}.$$

Let  $1 < q < p < 2$ . Let  $0 < \theta < 1$  be such that  $(1 - \theta)/q + \theta/2 = 1/p$ . By Hölder's inequality,

$$d_{p,f} \leq d_{q,f}^{1-\theta} d_{2,f}^\theta.$$

Thus if  $A_0$  has  $d_{q,f}$ -diameter  $\leq r_0$  and if  $A_1$  has  $d_{2,f}$ -diameter  $\leq r_1$ , then  $A_0 \cap A_1$  has  $d_{p,f}$ -diameter  $\leq r_0^{1-\theta} r_1^\theta$ . From this it is clear (taking intersections) that  $G$  can be covered by  $2^n \times 2^n$  sets with  $d_{p,f}$ -diameter  $\leq (e_n(d_{q,f}))^{1-\theta} (e_n(d_{2,f}))^\theta$ . In other words

$$e_{2n}(d_{p,f}) \leq (e_n(d_{q,f}))^{1-\theta} (e_n(d_{2,f}))^\theta.$$

Therefore by Hölder

$$\sum_0^\infty e_{2n}(d_{p,f}) n^{-1/p'} \leq \sum_0^\infty (e_n(d_{q,f}) n^{-1/q'})^{1-\theta} (e_n(d_{2,f}) n^{-1/2})^\theta \leq (\Sigma_q(f))^{1-\theta} (\Sigma_2(f))^\theta.$$

But since the numbers  $e_n(d_{p,f})$  (and also  $e_n(d_{p,f}) n^{-1/p'}$ ) are obviously non-increasing we have  $\sum_0^\infty e_n(d_{p,f}) n^{-1/p'} \leq 2 \sum_0^\infty e_{2n}(d_{p,f}) (2n)^{-1/p'}$  and hence we obtain

$$\Sigma_p(f) \leq 2^{1/p} (\Sigma_q(f))^{1-\theta} (\Sigma_2(f))^\theta.$$

Lastly, we invoke a result from approximation theory, that tells us that for any  $1 < q < \infty$  there is a constant  $\beta_q$  such that

$$\Sigma_q(f) \leq \beta_q \sum_{\pi \in \widehat{G}} |\widehat{f}(\pi)|.$$

See [33] or [7, Prop. 2, p. 142]. Since  $\Sigma_p(f)$  is equivalent to  $\mathcal{I}_p(f)$ , this gives us (4.17).  $\square$

**Theorem 4.13** (Sidon versus central  $\Lambda(p)$ -sets). *Let  $\Lambda \subset \widehat{G}$ . Recall  $\mathcal{G} = \prod_{\pi \in \Lambda} U(d_\pi)$ . Consider the following assertions in addition to (i) and (ii) in Theorem 4.10.*

(iii) *Same as (ii) for all (central) functions  $f$  of the form  $f = \sum_{\pi \in A} d_\pi \chi_\pi$  where  $A \subset \Lambda$  is an arbitrary finite subset.*

(iii)' *There is a constant  $C$  such that for any even integer  $2 \leq p < \infty$  and any finite subset  $A \subset \Lambda$  we have*

$$\left\| \sum_{\pi \in A} d_\pi \chi_\pi \right\|_p \leq C \sqrt{p} \left\| \sum_{\pi \in A} d_\pi \chi_\pi \right\|_2 = C \sqrt{p} \left( \sum_{\pi \in A} d_\pi^2 \right)^{1/2}.$$

(iv) *For any  $0 < \delta < 1$  there is  $0 < \beta < \infty$  such that for any finite subset  $A \subset \Lambda$  we have*

$$m_G(\{t \in G \mid \sum_{\pi \in A} d_\pi \Re(\chi_\pi) > \delta \sum_{\pi \in A} d_\pi^2\}) \leq e \exp -(\beta \sum_{\pi \in A} d_\pi^2)$$

(v) *There are  $0 < \delta < 1$  and  $0 < \beta < \infty$  such that for any finite subset  $A \subset \Lambda$  we have*

$$m_G(\{t \in G \mid \sum_{\pi \in A} d_\pi \Re(\chi_\pi) > \delta \sum_{\pi \in A} d_\pi^2\}) \leq e \exp -(\beta \sum_{\pi \in A} d_\pi^2)$$

(vi) *There is a constant  $C$  such that for any finite  $A \subset \Lambda$*

$$\sum_{\pi \in A} d_\pi^2 \leq C \int_{\mathcal{G}} \sup_{g \in G} \left| \sum_{\pi \in A} d_\pi \operatorname{tr}(u_\pi \pi(g)) \right| m_{\mathcal{G}}(du).$$

(vii) *There is  $0 < \delta < 1$  such that any finite subset  $A \subset \Lambda$  contains a further subset  $B \subset A$  with Sidon constant at most  $1/\delta$  and such that  $\sum_{\pi \in B} d_\pi^2 \geq \delta \sum_{\pi \in A} d_\pi^2$ .*

(viii) There is a constant  $C$  such that for any finite subset  $A \subset \Lambda$ , and any  $f \in L_2(G)$  with  $\widehat{f}$  supported in  $A$  we have

$$(4.18) \quad \|f\|_{\psi_2} \leq C \left( \sum_{\pi \in A} d_\pi^2 \right)^{1/2} \sup_{\pi \in A} \|\widehat{f}(\pi)\|.$$

Then (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii)  $\Leftrightarrow$  (iii)'  $\Rightarrow$  (iv)  $\Rightarrow$  (v)  $\Rightarrow$  (vi)  $\Rightarrow$  (vii)  $\Rightarrow$  (viii). Moreover, (viii)  $\Rightarrow$  (i) if  $G$  is Abelian, or more generally if the dimensions  $\{d_\pi \mid \pi \in \Lambda\}$  are uniformly bounded.

*Proof.* Recall (i)  $\Leftrightarrow$  (ii) by Theorem 4.10, (ii)  $\Rightarrow$  (iii) is trivial and (iii)  $\Leftrightarrow$  (iii)' follows from (4.3). Assume (iii). In the rest of the proof, we follow [38] except for the correction indicated in Remark 4.14. Let  $A \subset \Lambda$  be a finite subset. Let  $N(A) = \sum_{\pi \in A} d_\pi^2$ . (Incidentally,  $N(A)$  is the Plancherel measure of  $A$ .) By (4.3)  $\|\sum_{\pi \in A} d_\pi \chi_\pi\|_{L_{\psi_2}} \leq CC_2(N(A))^{1/2}$ . Therefore for any  $\delta > 0$  we have

$$m_G(\{t \in G \mid |\sum_{\pi \in A} d_\pi \chi_\pi| > \delta N(A)\}) \leq e \exp(-(\delta^2 N(A)/(CC_2)^2)).$$

A fortiori, (iv) holds and (iv)  $\Rightarrow$  (v) is trivial.

Assume (v). Let  $A \subset \Lambda$  be a finite subset. Consider the random Fourier series

$$S_A(g) = \sum_{\pi \in A} d_\pi \operatorname{tr}(u_\pi \pi(g))$$

defined for  $u = (u_\pi) \in \mathcal{G}$  as in Remark 4.7. The associated metric  $d_A$  is given by

$$d_A(g, g')^2 = \sum_{\pi \in A} d_\pi \operatorname{tr}|\pi(g) - \pi(g')|^2 = 2 \sum_{\pi \in A} d_\pi^2 - 2 \sum_{\pi \in A} d_\pi \Re(\chi_\pi(g'g^{-1})).$$

Therefore

$$\{g \in G \mid d_A(g, 1) < \varepsilon N(A)^{1/2}\} = \{g \in G \mid \sum_{\pi \in A} d_\pi \Re(\chi_\pi(g)) > (1 - \varepsilon^2/2)N(A)\}.$$

Thus (v) implies that for some  $\varepsilon > 0$  (chosen so that  $1 - \varepsilon^2/2 = \delta$ ) we have

$$m_G(\{g \in G \mid d_A(g, 1) < \varepsilon N(A)^{1/2}\}) \leq \exp(1 - \beta N(A)).$$

Then by (4.8) we find

$$\varepsilon N(A)^{1/2}(\beta N(A) - 1)^{1/2} \leq cc' \mathbb{E} \sup_{g \in G} |S_A(g)|,$$

from which (vi) is immediate.

Assume (vi). Let  $V_A$  denote the linear space formed of all random functions of the form  $F(u)(g) = \sum_{\pi \in A} d_\pi \operatorname{tr}(u_\pi a_\pi \pi(g))$  with  $a_\pi$  arbitrary in  $M_{d_\pi}$ . Let  $\|\cdot\|_A$  be the norm induced on it by  $L_1(\mathcal{G}; C(G))$ , i.e.

$$\|F\|_A = \int_{\mathcal{G}} \sup_{g \in G} |F(u)(g)| m_{\mathcal{G}}(du).$$

With  $S_A$ ,  $N(A)$  as before, (v) tells us that

$$\|S_A\|_A \geq N(A)/C.$$

By Hahn-Banach, there is  $y \in A^*$  with  $\|y\|_A^* \leq 1$  such that  $\langle y, S_A \rangle = \|S_A\|_A \geq N(A)/C$ . Identifying  $y \in A^*$  with a family  $(y_\pi)$  with  $y_\pi \in M_{d_\pi}$  ( $\pi \in A$ ), we may assume that  $\langle y, F \rangle = \sum_{\pi \in A} d_\pi \operatorname{tr}(y_\pi a_\pi)$ . Then  $\langle y, S_A \rangle = \sum_{\pi \in A} d_\pi \operatorname{tr}(y_\pi)$ . Moreover, by the translation invariance of the norm  $\|\cdot\|_A$  (on



$\mathcal{G}$  and on  $G$ ), for any fixed  $u', g'$  we have  $\|F\|_A = \|F(\cdot u')(g' \cdot)\|_A$ . By duality this implies  $\|y\|_A^* = \|(\pi(g')y_\pi u'_\pi)\|_A^*$ , and hence

$$\left\| \left( \int \pi(g')y_\pi \pi(g'^{-1})m_G(dg') \right) \right\|_A^* \leq 1.$$

But since the  $\pi$ 's are irreducible,  $\int \pi(g')y_\pi \pi(g'^{-1})m_G(dg') = I_{d_\pi} \text{tr}(y_\pi)/d_\pi$ , and hence

$$\|(I_{d_\pi} \text{tr}(y_\pi)/d_\pi)\|_A^* \leq 1,$$

which means that for any  $F$

$$|\sum_{\pi \in A} \text{tr}(y_\pi) \text{tr}(a_\pi)| \leq \|F\|_A.$$

Since  $\|F\|_A$  is invariant if we replace  $a_\pi$  by  $|a_\pi| |\text{tr}(y_\pi)| (\text{tr}(y_\pi))^{-1}$  we also have

$$(4.19) \quad |\sum_{\pi \in A} |\text{tr}(y_\pi)| |\text{tr}(a_\pi)| \leq \|F\|_A.$$

In particular, in the case  $F(u)(g) = d_\pi \text{tr}(u_\pi \pi(g))$  for some  $\pi \in A$ , this implies

$$(4.20) \quad |d_\pi \text{tr}(y_\pi)| \leq d_\pi^2.$$

Now recalling that  $\langle y, S_A \rangle = \|S_A\|_A \geq N(A)/C$  we have  $\sum_{\pi \in A} d_\pi \text{tr}(y_\pi) \geq N(A)/C$ , and hence there is a subset  $B \subset A$  (namely  $B = \{\pi \mid |\text{tr}(y_\pi)| > d_\pi/2C\}$ ) such that  $|\sum_{\pi \in B} d_\pi \text{tr}(y_\pi)| \geq N(A)/2C$  and  $|\text{tr}(y_\pi)| > d_\pi/2C$  for any  $\pi \in B$ . By (4.20)

$$\sum_{\pi \in B} d_\pi^2 \geq |\sum_{\pi \in B} d_\pi \text{tr}(y_\pi)| \geq N(A)/2C,$$

and by (4.19) the randomly Sidon constant of  $B$  is at most  $2C$ , so that (vii) holds by Corollary 3.7. Assume (vii). Let  $N(A) = \sum_{\pi \in A} d_\pi^2$ . We will show that there is  $C_\delta$  depending only on the  $\delta$  appearing in (vii) such that for any finite subset  $A \subset \Lambda$ , and any  $f \in L_2(G)$  with  $\hat{f}$  supported in  $A$  we have

$$(4.21) \quad \|f\|_{\psi_2} \leq C_\delta N(A)^{1/2} \sup_{\pi \in A} \|\hat{f}(\pi)\|.$$

To prove this we may assume that  $\Lambda$  is finite. Let  $C_\Lambda$  be the smallest constant for which (4.21) holds for all  $A \subset \Lambda$ .

Fix  $A \subset \Lambda$  and let  $B \subset A$  as in (vii). Let  $f \in L_2(G)$  with  $\hat{f}$  supported in  $A$ . We will show that (vii) implies that

$$(4.22) \quad \|f\|_{\psi_2} \leq C'_\delta N(A)^{1/2} \sup_{\pi \in A} \|\hat{f}(\pi)\| + C_\Lambda (1 - \delta)^{1/2} N(A)^{1/2} \sup_{\pi \in A} \|\hat{f}(\pi)\|,$$

where  $C'_\delta$  is a constant depending only on  $\delta$ . Indeed, by the triangle inequality we have

$$\|f\|_{\psi_2} \leq \left\| \sum_{\pi \in B} d_\pi \text{tr}({}^t \hat{f}(\pi) \pi) \right\|_{\psi_2} + \left\| \sum_{\pi \in A \setminus B} d_\pi \text{tr}({}^t \hat{f}(\pi) \pi) \right\|_{\psi_2}.$$

Note

$$\left\| \sum_{\pi \in B} d_\pi \text{tr}({}^t \hat{f}(\pi) \pi) \right\|_2 = \left( \sum_{\pi \in B} d_\pi \text{tr}(|\hat{f}(\pi)|^2) \right)^{1/2} \leq N(B)^{1/2} \sup_{\pi \in B} \|\hat{f}(\pi)\| \leq N(A)^{1/2} \sup_{\pi \in A} \|\hat{f}(\pi)\|.$$

Thus, by Theorem 4.10 applied to the set  $B$  there is  $C'_\delta$  such that

$$\left\| \sum_{\pi \in B} d_\pi \text{tr}({}^t \hat{f}(\pi) \pi) \right\|_{\psi_2} \leq C'_\delta \left\| \sum_{\pi \in B} d_\pi \text{tr}({}^t \hat{f}(\pi) \pi) \right\|_2 \leq C'_\delta N(A)^{1/2} \sup_{\pi \in A} \|\hat{f}(\pi)\|,$$

and by definition of  $C_\Lambda$  we have

$$\left\| \sum_{\pi \in A \setminus B} d_\pi \text{tr}({}^t \widehat{f}(\pi) \pi) \right\|_{\psi_2} \leq C_\Lambda N(A \setminus B)^{1/2} \sup_{A \setminus B} \|\widehat{f}(\pi)\| \leq C_\Lambda (1 - \delta)^{1/2} N(A)^{1/2} \sup_A \|\widehat{f}(\pi)\|,$$

from which (4.22) is immediate.

Equivalently, (4.22) means  $C_\Lambda \leq C'_\delta + C_\Lambda (1 - \delta)^{1/2}$  and hence

$$C_\Lambda \leq (1 - (1 - \delta)^{1/2}) C'_\delta,$$

which proves (4.21). Thus we have proved (vii)  $\Rightarrow$  (viii).

Now assume (viii) but *we also assume that  $d_\pi = 1$  for all  $\pi \in \Lambda$* . Let us denote by  $\ell_{2,1}(\Lambda)$  the classical Lorentz space of scalar sequences indexed by  $\Lambda$ . Explicitly, given a scalar family  $a = (a_\pi)$  (say, tending to 0 at  $\infty$ ), we denote by  $(a_n^*)$  the non-increasing rearrangement of the numbers  $\{|\widehat{f}(\pi)| \mid \pi \in \Lambda\}$ . Let

$$\|a\|_{2,1} = \sum_1^\infty a_n^*/n^{1/2}.$$

The space  $\ell_{2,1}(\Lambda)$  is defined as formed of those  $a$  for which this sum is finite. It is well known that  $\|\cdot\|_{2,1}$  is equivalent to a norm on  $\ell_{2,1}(\Lambda)$  (we will not use this). Note that (4.18) simply means  $\|f\|_{\psi_2} \leq C|A|^{1/2} \sup_A |\widehat{f}(\pi)|$ . This implies

$$\|f\|_{\psi_2} \leq 3C \|(\widehat{f}(\pi))\|_{2,1}.$$

Indeed, using the disjoint decomposition of  $\Lambda$  associated to  $\{a_n^*\} = \cup_{k \geq 0} \{a_n^* \mid 2^k \leq n < 2^{k+1}\}$ , we find

$$\|f\|_{\psi_2} \leq C \sum_{k \geq 0} 2^{k/2} a_{2^k}^* \leq 3C \sum_1^\infty a_n^*/n^{1/2} = 3C \|(\widehat{f}(\pi))\|_{2,1}.$$

Let  $1 < p < 2$ . Let  $2 < p' < \infty$  be the conjugate, so that  $1/p + 1/p' = 1$ . Let

$$\|(\widehat{f}(\pi))\|_p = \left( \sum_\Lambda |\widehat{f}(\pi)|^p \right)^{1/p}.$$

We claim that there is a constant  $\chi$  depending only on  $p$  and  $C$  such that for any  $f$  with  $\widehat{f}$  supported in  $\Lambda$

$$(4.23) \quad \|f\|_{\psi_{p'}} \leq \chi \|(\widehat{f}(\pi))\|_p.$$

This follows from a rather simple interpolation argument. Indeed, we have  $\|(\widehat{f}(\pi))\|_p = (\sum a_n^{*p})^{1/p}$ . Fix a number  $N \geq 1$ . Let  $f = f_0 + f_1$  be the decomposition of  $f$  associated to  $\{a_n^*\} = \{a_n^* \mid 1 \leq n \leq N\} \cup \{a_n^* \mid n > N\}$ , so that

$$\|f_0\|_\infty \leq \sum_1^N a_n^* \text{ and } \|f_1\|_{\psi_2} \leq 3C \sum_{n > N} a_n^*/n^{1/2}.$$

By homogeneity we may assume  $\|(\widehat{f}(\pi))\|_p = 1$ . Then  $a_n^* \leq n^{-1/p}$  for all  $n \geq 1$ . Therefore  $\sum_1^N a_n \leq \sum_1^N n^{-1/p} \leq p' N^{1/p'}$  and  $\sum_{n > N} a_n^*/n^{1/2} \leq \sum_{n > N} n^{-1/p-1/2} \leq \frac{2p'}{p'-2} N^{1/p'-1/2}$ .

Let  $c = p' N^{1/p'}$  so that  $\|f_0\|_\infty \leq c$ . We have

$$\mathbb{P}(\{|f| > 2c\}) \leq \mathbb{P}(\{|f_0| > c\}) + \mathbb{P}(\{|f_1| > c\}) = \mathbb{P}(\{|f_1| > c\}).$$

But we have

$$\mathbb{P}(\{|f_1| > c\}) \leq e \exp -c^2 / \|f_1\|_{\psi_2}^2$$

and since  $\|f_1\|_{\psi_2} \leq 3C \frac{2p'}{p'-2} N^{1/p'-1/2} = 3C \frac{2p'}{p'-2} (c/p')^{1-p'/2}$  we find after substituting

$$\mathbb{P}(\{|f| > 2c\}) \leq \mathbb{P}(\{|f_1| > c\}) \leq e \exp -(\chi' c^{p'}),$$

where  $\chi'$  is a constant depending only on  $p$  and  $C$ . This has been established for  $c$ 's of the form  $c = p' N^{1/p'}$ , but it is easy to obtain all values by interpolating between two such values. From this, our claim (4.23) is now immediate (recall (iii)  $\Rightarrow$  (ii) in Lemma 4.1 and Remark 4.2). From this claim, we obtain that  $\Lambda$  is Sidon by Lemma 4.12. The case when the dimensions  $d_\pi$  are uniformly bounded by a fixed number  $D$  follows by a straightforward modification of the same argument (but all the resulting bounds will depend on  $D$ ). In any case, this shows that (viii)  $\Rightarrow$  (i) in the latter case.  $\square$

*Remark 4.14.* In [38] it is erroneously claimed that (viii)  $\Rightarrow$  (i) in full generality in the nonAbelian case. However we recently noticed that the proof has a serious gap, and we now believe that the result does not hold. Indeed, if  $\Lambda = \{\pi_n \mid n \in \mathbb{N}\}$  and if the dimensions of the representations in  $\Lambda$  form a sequence such that  $d_n^2 \geq d_1^2 + \dots + d_{n-1}^2$ , then the mere knowledge that the individual singletons  $\{\pi_n\}$  are Sidon with a fixed constant (Rider [48] called this “local Sidon property”) is sufficient to guarantee that (vii) holds, but it seems unlikely that this is enough to force  $\Lambda$  to be Sidon.

Although we state it in full generality, the next result is significant only if the dimensions of the irreps  $\pi_n$  are unbounded.

**Theorem 4.15** (Characterizing SubGaussian characters). *Let  $G_n$  be a sequence of compact groups, let  $\pi_n \in \widehat{G_n}$  be nontrivial irreps and let  $\chi_n = \chi_{\pi_n}$  as well as  $d_n = d_{\pi_n}$ . The following are equivalent.*

(i) *There is a constant  $C$  such that the singletons  $\{\pi_n\} \subset \widehat{G_n}$  are Sidon with constant  $C$ , i.e. we have*

$$\forall n \forall a \in M_{d_n} \quad \text{tr}|a| \leq C \sup_{g \in G} |\text{tr}(a\pi_n(g))|.$$

(ii) *There is a constant  $C$  such that*

$$\forall n \quad \|\chi_n\|_{\psi_2} \leq C.$$

(ii)' *There is  $\beta > 0$  such that*

$$\forall n \quad \int \exp(\beta |\chi_n|^2) dm_{G_n} \leq e.$$

(ii)'' *There is a constant  $C$  such that for any  $t \in \mathbb{R}$*

$$\forall n \quad \int \exp(t\chi_n - Ct^2) dm_{G_n} \leq 1.$$

(iii) *For each  $0 < \delta < 1$  there is  $0 < \theta < 1$  such that*

$$\forall n \quad m_{G_n}\{Re(\chi_n) > \delta d_n\} \leq e\theta^{d_n^2}.$$

(iii)' *For each  $0 < \delta < 1$  there is  $0 < \theta < 1$  and  $D > 0$  such that for any  $n$  with  $d_n > D$  we have*

$$m_{G_n}\{Re(\chi_n) > \delta d_n\} \leq \theta^{d_n^2}.$$

(iii)'' *There are  $0 < \delta < 1$  and  $0 < \theta < 1$  such that*

$$\forall n \quad m_{G_n}\{Re(\chi_n) > \delta d_n\} \leq e\theta^{d_n^2}.$$

(iv) There is a constant  $C$  such that

$$\forall n \quad d_n \leq C \int_{U(d_n)} \sup_{g \in G_n} |\text{tr}(u\pi_n(g))| m_{U(d_n)}(du).$$

*Proof.* Note that the properties (ii) (ii)' and (ii)'' are just reformulations of each other by Lemmas 4.1 and 4.3. Note that the content of (iii) and (iii)'' is void when  $e\theta^{d_n^2} \geq 1$ . Thus (iii)  $\Rightarrow$  (iii)'  $\Rightarrow$  (iii)'' are trivial. The implication (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii) is a special case of (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iv) in Theorem 4.13 and (iii)''  $\Rightarrow$  (iv) is a special case of (v)  $\Rightarrow$  (vi) in Theorem 4.13. Moreover, we may invoke the implication (vi)  $\Rightarrow$  (vii) in Theorem 4.13 for our special case of singletons. Then the Corollary boils down to the observation that if  $\Lambda$  is a singleton the implication (vii)  $\Rightarrow$  (i) in Theorem 4.13 trivially holds (take  $A = \Lambda$ , then necessarily  $B = \Lambda$ ).  $\square$

Although I never had concrete examples, I believed naively for many years that Theorem 4.15 could be applied to finite groups. To my surprise, Emmanuel Breuillard showed me that it is not so (and he pointed out Turing's paper [59] that already emphasized that general phenomenon, back in 1938). It turns out that, when the groups  $G_n$  are finite (or amenable as discrete groups), Theorem 4.15 can hold only if the dimensions  $d_n$  remain bounded. The reason lies in the presence of large Abelian subgroups with index of order  $\exp o(d_n^2)$ . The latter follows from the quantitative refinements in [61, 10] of a classical Theorem of Camille Jordan on finite linear groups. See the forthcoming paper [5] for details.

## 5. Some questions about best constants

We denote by  $A_p, B_p$  the best possible constants in the classical Khintchine inequalities. These inequalities say that for any scalar sequence  $x \in \ell_2$  we have

$$A_p(\sum |x_j|^2)^{1/2} \leq (\int |\sum \varepsilon_j x_j|^p d\mathbb{P})^{1/p} \leq B_p(\sum |x_j|^2)^{1/2}.$$

After much effort by many authors, the exact values of  $A_p, B_p$  were obtained by Szarek and Haagerup (see [21, 56]). Let  $p_0 = 1.87\dots$  be the unique solution in the interval  $]1, 2[$  of the equation  $2^{1/2-1/p} = \gamma_p$  (or explicitly  $\Gamma((p+1)/2) = \sqrt{\pi}/2$ ), then Haagerup (see [21]) proved :

$$(5.1) \quad A_p = 2^{1/2-1/p} \quad 0 < p \leq p_0,$$

$$(5.2) \quad A_p = \gamma_p \quad p_0 \leq p \leq 2,$$

$$(5.3) \quad B_p = \gamma_p \quad 2 \leq p < \infty.$$

The bounds  $A_p \leq \gamma_p$  for  $p \leq 2$  and  $B_p \geq \gamma_p$  for  $p \geq 2$  are easy consequences of the Central Limit Theorem, applied to  $\lim_{n \rightarrow \infty} (\varepsilon_1 + \dots + \varepsilon_n)/\sqrt{n}$ . The bound  $A_p \leq 2^{1/2-1/p}$  is immediate by considering the function  $(\varepsilon_1 + \varepsilon_2)/\sqrt{2}$ .

For the complex analogue of these inequalities, the best constants are also known: if we replace the sequence  $(\varepsilon_n)$  (independent choices of signs) by an i.i.d. sequence  $(z_n)$  uniformly distributed over  $\{z \in \mathbb{C} \mid |z| = 1\}$ , then the same inequalities hold but now the best constants, that we denote  $A_p[\mathbb{T}], B_p[\mathbb{T}]$ , are  $A_p[\mathbb{T}] = \gamma_p^{\mathbb{C}}$  if  $1 \leq p \leq 2$  and  $B_p[\mathbb{T}] = \gamma_p^{\mathbb{C}}$  if  $p \geq 2$ , where  $\gamma_p^{\mathbb{C}}$  is the  $L_p$ -norm of a standard complex-valued Gaussian variable normalized in  $L_2$ . Indeed, in analogy with

Haagerup's result, Sawa [53, 54] proved that there is a phase transition at a number  $p_0^{\mathbb{C}}$ , but now  $0 < p_0^{\mathbb{C}} = 0.475... < 1!$

Let  $G$  be a matrix group, such as  $U(d), SU(d), O(d), SO(d)$ . Let  $\pi_n : G^{\mathbb{N}} \rightarrow G$  denote the  $n$ -th coordinate. Let  $E[G]$  be the linear span of the matrix coefficients of  $\Lambda = \{\pi_n \mid n \in \mathbb{N}\}$ . Thus a typical element of  $E[G]$  can be written as a finite sum  $f = \sum \text{tr}(\pi_n x_n)$ , where  $(x_n)$  is a finitely supported family in  $M_d$ . Then  $\|f\|_2 = (d^{-1} \sum \text{tr}|x_n|^2)^{1/2}$ .

We denote by  $A_p[G], B_p[G]$  the best (positive) constants  $A, B$  in the following inequality

$$(5.4) \quad \forall f \in E[G] \quad A\|f\|_2 \leq \|f\|_p \leq B\|f\|_2.$$

Let  $\Gamma^u = \prod_{d \geq 1} U(d)$ ,  $\Gamma^o = \prod_{d \geq 1} O(d)$ . We set  $\mathcal{G}^u = (\Gamma^u)^{\mathbb{N}}$  and  $\mathcal{G}^o = (\Gamma^o)^{\mathbb{N}}$ . We define similarly  $\mathcal{G}^{su}$  and  $\mathcal{G}^{so}$ .

**Problem:** Let  $1 \leq p \neq 2 < \infty$ . What are the values of  $A_p[G], B_p[G]$  for  $G = U(d)$  for  $d > 1$  ? Same question for  $SU(d), O(d), SO(d)$ .

It is natural to consider also the best constants  $A_p^c[G], B_p^c[G]$  for which (5.4) holds for all central functions  $f$ , i.e. all  $f$  of the form  $f = \sum \text{tr}(\pi_n) x_n$  where  $(x_n)$  is a finitely supported family in  $\mathbb{C}$ . Another natural question is to find the best  $A_p[G], B_p[G]$  for  $G = \mathcal{G}^u$  and similarly when  $G$  is either  $\mathcal{G}^o, \mathcal{G}^{su}$  or  $\mathcal{G}^{so}$ .

The constants  $A_p[\mathcal{G}^u], B_p[\mathcal{G}^u]$  can equivalently be viewed as the best constants in (5.4) when  $f$  is any finite sum of the form

$$f(\omega) = \sum \text{tr}(\rho_n(\omega) x_n) \quad (x_n \in M_{d_n})$$

where  $\Omega = \prod U(d_n)$  is equipped with its uniform (Haar) probability,  $\rho_n : \Omega \rightarrow U(d_n)$  is the  $n$ -th coordinate and  $(d_n)$  is an arbitrary sequence of integers (and similarly for  $o, su, so$ ). Then  $\|f\|_2 = (\sum d_n^{-1} \text{tr}|x_n|^2)^{1/2}$ .

Consider a (real or complex) Banach space  $B$ . Recall that a  $B$ -valued random variable  $X$  is called Gaussian if for any real linear form  $\xi : B \rightarrow \mathbb{R}$ , the real valued variable  $\xi(X)$  is Gaussian. By definition, the covariance of a  $B$ -valued random variable  $X$  is the bilinear form  $(\xi, \xi') \mapsto \mathbb{E}(\xi(X)\xi'(X))$ . Let  $g^{(d)}$  be a Gaussian random matrix with the same covariance as  $x \mapsto \pi_n(x)$  (the latter does not depend on  $n$ ), so that, by the central limit theorem (CLT in short),  $n^{-1/2}(\pi_1 + \dots + \pi_n)$  tends in distribution to  $g^{(d)}$ . In particular, When  $G = SO(d)$  or  $O(d)$  (resp.  $G = SU(d)$  or  $U(d)$ )  $n^{-1/2}(\text{tr}(\pi_1) + \dots + \text{tr}(\pi_n))$  tends in distribution to a standard real (resp. complex) Gaussian random variable normalized in  $L_2$ . It follows that  $B_p \geq B_p^c \geq \gamma_p^{\mathbb{R}}$  (resp.  $B_p \geq B_p^c \geq \gamma_p^{\mathbb{C}}$ ) for all  $p \geq 2$  and  $A_p \leq A_p^c \leq \gamma_p^{\mathbb{R}}$  (resp.  $A_p \leq A_p^c \leq \gamma_p^{\mathbb{C}}$ ) for all  $p \leq 2$ .

In [23, §36, p. 390] it is proved that

$$\forall p \in 2\mathbb{N} \quad B_p[\mathcal{G}^u] \leq 2((p/2)!)^{1/p}$$

with an improved bound for  $p = 4$  namely  $B_4[\mathcal{G}^u] \leq 2$ . A fortiori,  $B_4[U(d)] \leq 2$  for all  $d \geq 1$ . Since  $\gamma_4^{\mathbb{C}} = 2$  this implies

$$B_4[U(d)] = B_4^c[U(d)] = B_4[\mathcal{G}^u] = B_4^c[\mathcal{G}^u] = 2.$$

Hewitt and Ross quote [16] but they also credit Rider and quote another paper of his entitled "Continuity of random Fourier series" that apparently never appeared. Moreover, by a result due to Helgason [22]

$$A_1[\mathcal{G}^u] \geq 1/\sqrt{2}.$$

Let  $G = U(d)$  (resp.  $G = O(d)$ ). Let  $(g_n^{(d)})$  be an i.i.d. sequence of copies of  $g^{(d)}$ . Following [34], we describe in Lemma 4.4 a very general comparison principle showing that for some absolute constant

$C_0$  the family of coefficients  $\{\pi_n(i, j)\}$  is the image of  $\{g_n^{(d)}(i, j)\}$  under a positive operator of norm at most  $C_0$  on  $L_p$ . In the proof of Lemma 4.4 we show this with

$$C_0 \leq \chi = \sup_d (d^{-1} \mathbb{E} \text{tr} |g^{(d)}|)^{-1} < \infty,$$

but we do not know the best value of  $C_0$ . In any case, this reasoning implies

$$\forall p \geq 2 \quad B_p[U(d)] \leq (d^{-1} \mathbb{E} \text{tr} |g^{(d)}|)^{-1} \gamma_p^{\mathbb{C}} \text{ and } B_p[\mathcal{G}^u] \leq \chi \gamma_p^{\mathbb{C}},$$

and similarly for  $O(d)$  with the analogue of  $g^{(d)}$  that has real valued Gaussian entries.

*Remark 5.1.* Let  $G$  be a compact group, let  $\Lambda \subset \widehat{G}$ , and let  $E_\Lambda$  be the linear span of the matrix coefficients of the representations in  $\Lambda$ . Let  $A_p^\Lambda$  and  $B_p^\Lambda$  be the best constants for which (5.4) holds for any  $f \in E_\Lambda$ . Then, if  $p > 2$ ,  $B_p^\Lambda$  can be interpreted as the constant of  $\Lambda$  as a  $\Lambda(p)$ -set in Rudin's sense [51]. See [1] for a rather recent survey on  $\Lambda(p)$ -sets. A similar interpretation is valid for  $A_p^\Lambda$  and  $\Lambda(p)$ -sets when  $1 < p < 2$ , but “true” examples of such sets are lacking for  $1 < p < 2$ .

*Remark 5.2.* One can also ask what are the best constants in (5.4) with respect to the usual non-commutative  $L_p$ -spaces when  $f$  is in the linear span of free Haar unitaries in the sense of [60]. Now semicircular (or circular) variables replace the Gaussian ones, when invoking the CLT, so that  $B_p \geq \|x\|_p$  where  $x$  is a semicircular (or circular) variable in the sense of [60] normalized in  $L_2$  (note  $\|x\|_\infty = 2$ ). For these free Haar unitaries, Bożejko's inequality in [4] implies that for any even integer  $p = 2n$  we have  $B_{2n} = (\frac{1}{n+1} \binom{2n}{n})^{1/2n}$ . The latter number is again the  $L_p$ -norm of a “free Gaussian”, i.e. a semicircular variable normalized in  $L_2$ . In particular (for this see also Haagerup's [20]) we have  $B_p \leq 2$  for all  $p \geq 2$ . Related results appear in [46, Lemma 7].

See [6] for interesting results on this theme.

## 6. A new approach to Rider's spectral gap

We now show how the new method presented in [44] yields another proof of Rider's spectral gap estimate. We do not obtain the nice precise description of the measure  $\mu_{k,n}$  that possesses the desired spectral gap property, as in Theorem 2.1, but we do get a more refined quantitative bound.

We need to recall the definitions of the projective and injective tensor product norms  $\|\cdot\|_\wedge$  and  $\|\cdot\|_\vee$  on the algebraic tensor product  $L_1(m_1) \otimes L_1(m_2)$  of two arbitrary  $L_1$ -spaces. Let  $T = \sum x_j \otimes y_j \in L_1(m_1) \otimes L_1(m_2)$ . Then

$$\|T\|_\wedge = \int |\sum x_j(t_1) y_j(t_2)| dm_1(t_1) dm_2(t_2)$$

$$\|T\|_\vee = \sup\{|\sum \langle x_j, \psi_1 \rangle \langle y_j, \psi_2 \rangle| \mid \|\psi_1\|_\infty \leq 1, \|\psi_2\|_\infty \leq 1\}.$$

Let  $(d_k)_{k \in I}$  be an arbitrary collection of integers. Let  $G = \prod_{k \in I} U(d_k)$ . Let  $u \mapsto u_k \in U(d_k)$  denote the coordinates on  $G$ . We know that the family  $\{d_k^{1/2} u_k(i, j)\}$  is subGaussian (see Lemma 4.4 or (i)  $\Rightarrow$  (ii) in Theorem 4.10). Let

$$S = \sum_{k, i, j} (d_k^{1/2} u_k(i, j)) \otimes (d_k^{1/2} u_k(j, i)).$$

Actually, by Lemma 4.4, in the terminology of [44], the family  $\{d_k^{1/2} u_k(i, j)\}$  is  $C_0$ -dominated by  $\{d_k^{1/2} g_k(i, j)\}$ . Therefore, by [44, Theorem 1.10], for any  $0 < \varepsilon < 1$  there is a decomposition

$$S = t + r$$

for some  $t, r \in L_1(G) \otimes L_1(G)$  satisfying

$$\|t\|_\wedge \leq w(\varepsilon) \quad \text{and} \quad \|r\|_\vee \leq \varepsilon,$$

where  $w(\varepsilon)$  depends only on  $\varepsilon$  and  $w(\varepsilon) = O(\log(1/\varepsilon))$  when  $\varepsilon \rightarrow 0$ .

Consider the mapping  $P : L_1(G) \otimes L_1(G) \rightarrow L_1(G)$  defined by  $P(x \otimes y) = x * y$ .

A simple verification shows that since  $u_k = u_k * u_k$  or equivalently  $u_k(i, j) = \sum_\ell u_k(i, \ell) * u_k(\ell, j)$

$$P(S) = \sum_k d_k \sum_{i,j} u_k(i, j) * u_k(j, i) = \sum_k d_k \sum_i u_k(i, i) = \sum_k d_k \text{tr}(u_k).$$

Moreover, for any  $t, r \in L_1(G) \otimes L_1(G)$  we have

$$\|P(t)\|_1 \leq \|t\|_\wedge$$

and

$$\|P(r)\|_* \leq \|r\|_\vee$$

where

$$\forall f \in L_1(G) \quad \|f\|_* = \sup_{\pi \in \widehat{G}} \|\widehat{f}(\pi)\|.$$

Indeed, note  $\|P(f)\|_* = \|T_{P(f)}\|_{B(L_2(G))}$  where  $T_{P(f)}$  is the convolutor  $x \mapsto x * P(f)$ . Then by a well known consequence of Grothendieck's theorem (obtained using translation invariance), there is a constant  $K$  such that

$$(K)^{-1} \|T_{P(f)}\|_{B(L_2(G))} \leq \|T_{P(f)}\|_{B(L_\infty(G), L_1(G))} = \|f\|_\vee.$$

Here  $K$  is the complex Grothendieck constant. Actually (see [43])  $K$  is not really needed here in view of the bound  $\|r\|_{\gamma_2^*} \leq \varepsilon$  directly obtained in [44]). Indeed, if  $f = \sum x_k \otimes y_k$  we have for any  $\varphi, \psi$  in  $L_\infty(G)$   $|\sum \langle \varphi, x_k \rangle \langle \psi, y_k \rangle| \leq \|f\|_\vee \|\varphi\|_\infty \|\psi\|_\infty$  and hence by a suitable averaging (replacing  $\varphi, \psi$  by suitable translates)

$$\sup_{s, t \in G} |\sum (\varphi * x_k)(s) (y_k * \psi)(t)| \leq K \|f\|_\vee \|\varphi\|_2 \|\psi\|_2$$

and hence

$$\sup_{t \in G} |\sum \varphi * (\sum x_k * y_k) * \psi(t)| \leq K \|f\|_\vee \|\varphi\|_2 \|\psi\|_2$$

from which  $\|P(f)\|_* = \|\sum x_k * y_k\|_* \leq K \|f\|_\vee$  follows immediately.

Thus we obtain

**Theorem 6.1.** *If the index set  $I$  is finite there is a decomposition  $\sum_{k \in I} d_k \text{tr}(u_k) = T + R$  with  $T, R \in L_1(G)$  such that  $\|T\|_1 \leq w(\varepsilon)$  and  $\|R\|_* \leq K\varepsilon$ . If  $I$  is infinite there is a similar decomposition within formal Fourier series with  $T \in M(G)$  such that  $\|T\|_{M(G)} \leq w(\varepsilon)$  and  $\|R\|_* \leq K\varepsilon$ .*

Let  $\pi_k(u) = u_k$  for any  $u \in G$ . Note  $\widehat{T}(\pi_k) = I - \widehat{R}(\pi_k)$ . Thus, if (say)  $K\varepsilon < 1/2$  then  $\|\widehat{T}(\pi_k) - I\| \leq 1/2$  and hence  $\|(\widehat{T}(\pi_k))^{-1}\| \leq 2$ . Since the set  $\Lambda = \{\pi_k\}$  is Sidon with constant = 1, the argument in Remark 3.9 shows:

**Corollary 6.2.** *For any  $\varepsilon < (2K)^{-1}$  there is a measure  $\mu \in M(G)$  with  $\|\mu\|_{M(G)} \leq 2w(\varepsilon)$  such that  $\widehat{\mu}(\pi_k) = I$  for all  $k$  and  $\sup_{\pi \notin \{\pi_k\}} \|\widehat{\mu}(\pi)\| \leq 2\varepsilon$ .*

The preceding proof yields the estimate  $w(\varepsilon) = O(\log(1/\varepsilon))$  that does not seem accessible by Rider's original approach. This logarithmic bound follows from [35, Lemma 3]. See [44, Remark 1.13] for a detailed deduction.

## References

- [1] J. Bourgain, Sidon sets and Riesz products. *Ann. Inst. Fourier (Grenoble)* 35 (1985), 137–148.
- [2] J. Bourgain,  $\Lambda_p$ -sets in analysis: results, problems and related aspects. *Handbook of the geometry of Banach spaces*, Vol. I, 195–232, North-Holland, Amsterdam, 2001.
- [3] J. Bourgain and M. Lewko, Sidonicity and variants of Kaczmarz’s problem, preprint, arxiv, April 2015.
- [4] M. Bożejko, On  $\Lambda(p)$  sets with minimal constant in discrete noncommutative groups, *Proc. of the Amer. Math. Soc.* 51 (1975), 407–412.
- [5] E. Breuillard and G. Pisier, Random unitaries and amenable linear groups, in preparation.
- [6] A. Buchholz, Optimal constants in Khintchine type inequalities for Fermions, Rademachers and  $q$ -Gaussian operators, *Bull. Polish Acad. Sci. Math.* 53 (2005), 315–321.
- [7] B. Carl, Entropy numbers of diagonal operators with an application to eigenvalue problems. *J. Approx. Theory* 32 (1981) 135–150.
- [8] C. Cecchini, Lacunary Fourier series on compact Lie groups. *J. Funct. Anal.* 11 (1972) 191–203.
- [9] S. Chevet, Séries de variables aléatoires gaussiennes à valeurs dans  $E \otimes_\varepsilon F$ , applications aux espaces de Wiener abstraits. Séminaire sur la géométrie des espaces de Banach 1977-1978, École Polytechnique, Exp. XIX, 1978. (available on [www.numdam.org](http://www.numdam.org)).
- [10] M. Collins, On Jordan’s theorem for complex linear groups. *J. Group Theory* 10 (2007), 411–423.
- [11] J. Faraut, *Analyse sur les groupes de Lie*. Calvage & Mounet, 2006.
- [12] A. Figà-Talamanca, Random Fourier series on compact groups. *Theory of Group Representations and Fourier Analysis (C.I.M.E., II Ciclo, Montecatini Terme, 1970)* pp. 1–63 Edizioni Cremonese, Rome, 1971.
- [13] A. Figà-Talamanca and C. Nebbia, *Harmonic analysis and representation theory for groups acting on homogeneous trees*, Cambridge University Press, Cambridge, 1991.
- [14] A. Figà-Talamanca and M. Picardello, *Harmonic analysis on free groups*, Marcel Dekker, New York, 1983.
- [15] A. Figà-Talamanca and D. Rider, A theorem of Littlewood and lacunary series for compact groups. *Pacific J. Math.* 16 (1966) 505–514.
- [16] A. Figà-Talamanca and D. Rider, A theorem on random fourier series on noncommutative groups. *Pacific J. Math.* 21 (1967) 487–492.
- [17] W. Fulton, *Young tableaux*. Cambridge University Press, 1997.
- [18] C. Graham and K. Hare, *Interpolation and Sidon sets for compact groups*. Springer, New York, 2013. xviii+249 pp.
- [19] C. Graham and O.C. Mc Gehee, *Essays in commutative harmonic analysis*. Springer-Verlag, New York-Berlin, 1979.



- [20] U. Haagerup, An example of a non-nuclear  $C^*$ -algebra which has the metric approximation property, *Inventiones Mat.* **50** (1979), 279–293.
- [21] U. Haagerup, The best constants in the Khintchine inequality, *Studia Math.* **70** (1981), 231–283 (1982).
- [22] S. Helgason, Topologies of Group Algebras and a Theorem of Littlewood, *Trans. Amer. Math. Soc.* **86** (1957), 269–283.
- [23] E. Hewitt and K. Ross, *Abstract harmonic analysis, Volume II, Structure and Analysis for Compact Groups, Analysis on Locally Compact Abelian Groups*, Springer, Heidelberg, 1970.
- [24] M. Hutchinson, Local  $\Lambda$  sets for profinite groups, *Pacific J. Math.* **80** (1980) 81–88.
- [25] J. P. Kahane, *Séries de Fourier absolument convergentes*, Springer, 1970.
- [26] J. P. Kahane, *Some random series of functions. Second edition*, Cambridge University Press, 1985.
- [27] M. Ledoux, *The concentration of measure phenomenon*, Mathematical Surveys and Monographs, 89. American Mathematical Society, Providence, RI, 2001.
- [28] M. Ledoux and M. Talagrand, *Probability in Banach Spaces. Isoperimetry and Processes*, Springer-Verlag, Berlin, 1991.
- [29] F. Lehner, A characterization of the Leinert property. *Proc. Amer. Math. Soc.* **125** (1997), 3423–3431.
- [30] D. Li and H. Queffélec, *Introduction à l'étude des espaces de Banach*. Société Mathématique de France, Paris, 2004.
- [31] J. Lindenstrauss and H.P. Rosenthal, The  $\mathcal{L}_p$  spaces, *Israel J. Math.* **7** (1969), 325–349.
- [32] J. López and K.A. Ross, *Sidon sets*. Lecture Notes in Pure and Applied Mathematics, Vol. 13. Marcel Dekker, Inc., New York, 1975.
- [33] M.B. Marcus, The  $\varepsilon$ -entropy of some compact subsets of  $\ell_p$ . *J. Approx. Theory* **10** (1974) 304–312.
- [34] M.B. Marcus and G. Pisier, *Random Fourier series with Applications to Harmonic Analysis*. Annals of Math. Studies n°101, Princeton Univ. Press, 1981.
- [35] J.-F. Méla, Mesures  $\varepsilon$ -idempotentes de norme bornée. *Studia Math.* **72** (1982), 131–149.
- [36] W. A. Parker, Central Sidon and central  $\Lambda_p$  sets. *J. Austral. Math. Soc.* **14**, 62–74 (1972).
- [37] G. Pisier, Ensembles de Sidon et processus gaussiens. *C.R. Acad. Sc. Paris*, t. A **286** (1978) 671–674.
- [38] G. Pisier, De nouvelles caractérisations des ensembles de Sidon. *Advances in Maths. Supplementary studies*, vol 7B (1981) 685–726.
- [39] G. Pisier, Arithmetic characterizations of Sidon sets. *Bull. A.M.S.* (1983) **8**, 87–90.

- [40] G. Pisier, Probabilistic methods in the geometry of Banach spaces, Probability and analysis (Varenna, 1985), 167–241, *Lecture Notes in Math.* 1206, Springer-Verlag, Berlin, 1986.
- [41] G. Pisier, *The volume of Convex Bodies and Banach Space Geometry*. Cambridge University Press, 1989.
- [42] G. Pisier, Multipliers and lacunary sets in non amenable groups. *Amer. J. Math.* 117 (1995) 337–376.
- [43] G. Pisier, Grothendieck’s Theorem, past and present. *Bull. Amer. Math. Soc.* 49 (2012), 237–323.
- [44] G. Pisier, On uniformly bounded orthonormal Sidon systems, preprint, arxiv 2016. To appear in *Math. Res. Letters*.
- [45] A. Prasad, *Representation theory. A combinatorial viewpoint*. Cambridge University Press, Delhi, 2015.
- [46] E. Ricard and Q. Xu, A noncommutative martingale convexity inequality, *Annals of Probability* 44 (2016), 867–882.
- [47] D. Rider, Randomly continuous functions and Sidon sets. *Duke Math. J.* 42 (1975) 752–764.
- [48] D. Rider,  $SU(n)$  has no infinite local  $\Lambda_p$  sets. *Boll. Un. Mat. Ital.* (4) 12 (1975), 155–160.
- [49] D. Rider, Norms of characters and central  $\Lambda_p$  sets for  $U(n)$ . Conference on Harmonic Analysis (Univ. Maryland, College Park, Md., 1971), pp. 287–294. *Lecture Notes in Math.*, Vol. 266, Springer, Berlin, 1972.
- [50] D. Rider, Central lacunary sets. *Monatsh. Math.* 76 (1972), 328–338.
- [51] W. Rudin, Trigonometric series with gaps. *J. Math. and Mech.* 9 (1960) 203–227.
- [52] B. Sagan, *The symmetric group* Springer, Second edition, New-York, 2001.
- [53] J. Sawa, The best constant in the Khintchine inequality for complex Steinhaus variables, the case  $p = 1$ , *Studia Math.* 81 (1985) 105–126.
- [54] J. Sawa, Some remarks on the Khintchine inequality for complex Steinhaus variables.
- [55] R. Stanley, *Enumerative combinatorics, vol. 2*. Cambridge Univ. Press
- [56] S. Szarek, On the best constants in the Khinchine inequality, *Studia Math.* 58 (1976), 197–208.
- [57] M. Talagrand, Regularity of Gaussian processes. *Acta Math.*, 159 (1987), 99–149.
- [58] M. Talagrand, *Upper and Lower Bounds for Stochastic Processes*, Springer, Berlin, 2014.
- [59] A. Turing, Finite approximations to Lie groups, *Annals of Math.* 39 (1938), 105–111.
- [60] D. Voiculescu, K. Dykema and A. Nica, *Free random variables*, Amer. Math. Soc., Providence, RI, 1992.
- [61] B. Weisfeiler, Post-classification version of Jordan’s theorem on finite linear groups, *Proc. Natl. Acad. Sci. USA* 81 (1984), 5278–5279.

- [62] H. Weyl, *The classical groups*. Princeton Univ. Press, 1939. Reprinted by Dover.
- [63] D. C. Wilson, On the structure of Sidon sets. *Monatsh. Math.* 101 (1986), 67–74.